Docket No. 241199US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SATO

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: ENCRYPTION APPARATUS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**:

Application No.	**Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	**APPLICATION NUMBER**	**MONTH/DAY/YEAR**
Japan	2002-241367	August 22, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier

Registration No. 25,599

C. Irvin McClelland
Registration Number 21,124

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

S03P0993US00

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月２２日

出願番号
Application Number: 特願２００２－２４１３６７

[ST.10/C]: ［ＪＰ２００２－２４１３６７］

出願人
Applicant(s): ソニー株式会社

２００３年　６月１０日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４４９３６

【書類名】　特許願

【整理番号】　0290074001

【提出日】　平成14年 8月22日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

H04L　9/30

H04L　9/06

H04B　1/38

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐藤　英雄

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代理人】

【識別番号】　100110434

【弁理士】

【氏名又は名称】　佐藤　勝

【手数料の表示】

【予納台帳番号】　076186

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0011610

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　暗号化装置

【特許請求の範囲】

【請求項１】　公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、

公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、

前記公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、

前記ハッシュ値を格納する記憶手段とを備え、

少なくとも、前記ハッシュ値生成手段が前記記憶手段にアクセスするに際して、前記公開鍵暗号化処理手段における各種演算処理を制限すること

を特徴とする暗号化装置。

【請求項２】　前記公開鍵暗号化処理手段は、演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、

少なくとも、前記ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、前記公開鍵暗号化処理手段における前記レジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替えること

を特徴とする請求項１記載の暗号化装置。

【請求項３】　前記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

前記共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、前記公開鍵暗号化処理手段における前記レジスタ群と共用すること

を特徴とする請求項１記載の暗号化装置。

【請求項４】　前記共通鍵暗号化処理手段は、ＤＥＳ暗号化処理を行うこと

を特徴とする請求項３記載の暗号化装置。

【請求項５】　前記公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化

処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、

前記ハッシュ値生成手段は、前記ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、

前記公開鍵暗号化演算処理コア手段と、前記ハッシュ値演算処理コア手段とを共用すること

を特徴とする請求項１記載の暗号化装置。

【請求項６】　前記公開鍵暗号化演算処理コア手段における加算手段と、前記ハッシュ値演算処理コア手段における加算手段とを共用すること

を特徴とする請求項５記載の暗号化装置。

【請求項７】　前記公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、

前記ハッシュ値生成手段におけるバス切り替えスイッチを、前記公開鍵暗号化処理手段における前記バス切り替えスイッチと共用すること

を特徴とする請求項１記載の暗号化装置。

【請求項８】　前記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

前記共通鍵暗号化処理手段におけるバス切り替えスイッチを、前記公開鍵暗号化処理手段における前記バス切り替えスイッチと共用すること

を特徴とする請求項７記載の暗号化装置。

【請求項９】　前記ハッシュ値生成手段は、生成したハッシュ値を前記記憶手段に格納するに際して、前記公開鍵暗号化処理手段によって用いられるアドレスに該ハッシュ値を格納し、

前記公開鍵暗号化処理手段は、前記記憶手段に格納されたハッシュ値を読み出すこと

を特徴とする請求項１記載の暗号化装置。

【請求項１０】　前記公開鍵暗号化処理手段は、楕円曲線暗号化処理を行うこと

を特徴とする請求項１記載の暗号化装置。

【請求項１１】　前記ハッシュ値生成手段は、ＳＨＡ－１処理を行うこと

を特徴とする請求項１記載の暗号化装置。

【請求項１２】　通信機能を有する非接触型ＩＣカードに組み込まれていること

を特徴とする請求項１記載の暗号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、いわゆる公開鍵暗号化方式による暗号化処理を行う暗号化装置に関する。

【０００２】

【従来の技術】

近年、例えば、いわゆるインターネット等を利用した電子商取引やオンラインショッピングといった各種通信技術を利用した様々なサービスが普及しつつある。また、近年では、通信技術の進歩にともない、端末を介した通信技術のみならず、例えば、交通機関の料金徴収やいわゆる電子マネー等に利用するための通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイスも開発されている。

【０００３】

このような通信機能を有するカード状のデバイス（以下、非接触型ＩＣ（Integrated Circuit）カードという。）は、取り扱いの便宜等の観点から、少ない回路規模で構成されるとともに、極めて少ない電力消費で動作することができ、且つ高速な処理を行うことが求められる。

【０００４】

【発明が解決しようとする課題】

ところで、上述した非接触型ＩＣカードを用いたサービスにおいては、通常、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理が行われる。その際、非接触型ＩＣカードにおいては、処理の高速化が要求されることから、これらの機能をソフトウェアによって実装す

ると、高いクロックのＣＰＵ（Central Processing Unit）を要することとなり、実用的でない。そのため、非接触型ＩＣカードにおいては、これらの機能をソフトウェアによって実装するのではなく、ハードウェアによって実装するのが望ましい。

【０００５】

ここで、このようなハードウェアによって上述した機能を実装する非接触型ＩＣカードにおいては、電力消費を極力抑制するために、例えばいわゆるＤＥＳ（Data Encryption Standard）暗号化方式といった比較的少ない回路規模及び電力消費で実装することができるいわゆる共通鍵暗号化方式を採用するものが多かった。

【０００６】

しかしながら、暗号化及び復号に共通の鍵を用いる共通鍵暗号化方式は、鍵データの授受を行う必要があるといった観点から、不正な第三者による攻撃に弱いという問題がある。そのため、非接触型ＩＣカードにおいては、将来的に金融サービスに適用する場合等の問題が懸念されていた。

【０００７】

そのため、非接触型ＩＣカードを用いたサービスにおいては、非接触型ＩＣカードとして、例えばいわゆるＲＳＡ（Rivest-Shamir-Adleman）暗号化方式や楕円曲線暗号化方式（Elliptic Curve Cryptosystem；ＥＣＣ）といったように、暗号化と復号とに用いる鍵を異なるものとし、秘密に保つ必要がある共通鍵を特定の１人が持てばよいいわゆる公開鍵暗号化方式を採用したセキュリティの高いシステムが要求されつつあり、公開鍵を用いた署名生成及び署名検証を行う非接触型ＩＣカードの開発も多く試みられている。

【０００８】

しかしながら、公開鍵暗号化方式は、共通鍵暗号化方式に比べ、セキュリティ性が極めて向上するものの、演算量が非常に膨大となることから、これをハードウェアによって実装する際には、回路規模が数十倍に増大し、規模が増大した回路に供給する電力も必然的に増大することになる。特に、各演算処理が同時に行われた場合には、これら演算処理が行われる回路で消費される瞬時電力の増大を

招く。

【０００９】

そのため、このような公開鍵暗号化方式を採用した非接触型ＩＣカードにおいては、回路規模、消費電力、及びコストの面で十分な特性を得ることができなかった。特に、非接触型ＩＣカードにおいては、限られた電力の多くを、暗号化処理を行うための回路に供給する必要があり、通信距離が数ミリ程度と短いものしか実用化されていない実情である。さらに、瞬時電力が予め制限された電力を上回った場合には各種演算処理が停止し、再度演算処理がやり直されることとなり、非接触型ＩＣカードにおける処理の遅延化を招く問題も生じている。

【００１０】

図１４は、縦軸を消費電力Ｗ、横軸を処理時刻Ｔとし、各処理における消費電力、及びこれら消費電力が加算された非接触型ＩＣカード全体における消費電力を模式的に比較した図である。同図（Ａ）乃至（Ｃ）は、ゲート、算出されたハッシュ値が格納されるＡＬＵ－ＲＡＭ、及びＲＡＭのそれぞれにおける処理に際して消費される消費電力を個別に示した図であり、同図（Ｄ）はこれら各処理における消費電力を加算した該非接触型ＩＣカード全体の消費電力を示す図である。同図（Ａ）乃至（Ｃ）によれば、処理時刻t_0において、ゲート、ＡＬＵ　ＲＡＭ、及びＲＡＭにおいて同時に処理動作が行われ、これら各処理における消費電力が加算された該非接触型ＩＣカード全体の消費電力は、同図（Ｄ）に示すように制限電力を瞬間的に超える場合がある。非接触型ＩＣカード全体としての消費電力が制限電力を超えると、各種処理動作を停止した後、再度処理動作が行われることとなり、消費電力が制限電力を超える時点までに行われた各種処理が無駄なものとなる。

【００１１】

さらに、消費電力が制限電力を超える毎に再度処理動作が行われると、該非接触型ＩＣカードにおける処理を高速で行うことが難しくなり、各種処理を高速で行うことを求められる非接触型ＩＣカードでは重大な問題となる。特に、ＡＬＵ　ＲＡＭにアクセスするに際しては、２～３ｎｓｅｃの如き短時間に消費される瞬時電力が大きく、これと同時に他の処理動作が行われると非接触型ＩＣカード

全体の瞬時電力が制限電力を超え、各種処理動作に遅延が生じる。

【００１２】

このように、非接触型ＩＣカードにおいては、セキュリティの面で強固であり公開鍵暗号化方式を採用することが期待されているものの、供給可能な電力やチップサイズ等の制限があるだけでなく、実装することが極めて困難であるうえ、消費電力の制限により高速処理を行うことが困難であった。

【００１３】

よって、本発明は、このような実情に鑑みてなされたものであり、回路規模を削減し、瞬時電力が低減された状態のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】

上述した目的を達成する本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限することを特徴としている。消費電力が比較的大きい処理動作を行うに際して、他の動作を一時的に制限することにより瞬時電力を低減し、電力を限界値以下に消費電力を抑制することにより、各種処理動作を停止させることなく高速処理を行うことができる。

【００１５】

このような本発明にかかる暗号化装置においては、公開鍵暗号化処理手段が、演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、少なくとも、ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替える。従って、各種処理動作を行うハードウェアを時分割で動作させることにより、瞬時電力を低減

することができ、消費電力が制限電力を超えることにより処理動作が停止させられることがなく、高速処理を行うことが可能となる。

【００１６】

また、この本発明にかかる暗号化装置においては、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用する。

【００１７】

このような本発明にかかる暗号化装置においては、公開鍵暗号化処理手段が、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理コア手段と、ハッシュ値演算処理コア手段とを共用する。

【００１８】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化演算処理コア手段における加算手段と、ハッシュ値演算処理コア手段における加算手段とを共用する。

【００１９】

このような本発明にかかる暗号化装置は、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【００２０】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【００２１】

このような本発明にかかる暗号化装置は、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納するに際して、公開鍵暗号化処理手段によって用いられるアドレスに該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出す。

【００２２】

このような本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用する。

【００２３】

このような本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡す。

【００２４】

【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【００２５】

この実施の形態は、例えば、通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイス（以下、非接触型ＩＣ（Integrated Circuit）カードという。）等に適用することができるものであって、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理の機能を、ハードウェアによって実装した暗号化装置である。特に、この暗号化装置は、いわゆる公開鍵暗号化方式を採用するものであって、暗号処理を行うに際して生成されるハッシュ値を記憶させるときに、瞬時電力の増大を招くことがないようにその他の各種処理を制限し、瞬時電力が低減された状態のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とするものである。

【００２６】

さらに、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、瞬時電力を低減することができるとともに、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とするものである。

【００２７】

なお、以下では、説明の便宜上、暗号化装置は、公開鍵暗号化方式として、いわゆる楕円曲線暗号化方式（Elliptic Curve Cryptosystem；ＥＣＣ）を採用し、認証やディジタル署名等に用いるハッシュ関数として、いわゆるＳＨＡ－１（Secure Hash Algorithm-1）を用い、さらに、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の１つであるいわゆるＤＥＳ（Data Encryption Standard）暗号化方式を用いて生成するものとして説明する。すなわち、暗号化装置は、公開鍵暗号化方式の一連の信号処理として、少なくとも、これら楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理を行うものとして説明する。

【００２８】

まず、暗号化装置において、楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理を時分割で行うに際して各ハードウェアを共用するための概念について説明する。

【００２９】

まず、暗号化装置においては、楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用する。すなわち、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素は、機能分析的に分解すると、図１（Ａ）に概念を示すように、レジスタ群と楕円曲線演算処理コア回路とに大別することができ、レジスタ群が当該ハードウェア構成要素の半分程度を占める。また、ＳＨＡ－１処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、同図（Ｂ）に示すように、レジスタ群とＳＨＡ－１演算処理コア回路とに大別することができる。そこで、暗号化装置においては、同図（Ｃ）に示すように、楕円曲線暗号化処理及びＳＨＡ－１処理のそれぞれを行うためのハードウェ

ア構成要素としてのレジスタを共用する。さらに、ＤＥＳ暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、図示しないが、レジスタ群とＤＥＳ演算処理コア回路とに大別することができることから、暗号化装置においては、楕円曲線暗号化処理及びＳＨＡ－１処理に加え、ＤＥＳ暗号化処理を行うためのハードウェア構成要素としてのレジスタをも共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【００３０】

また、暗号化装置においては、ＳＨＡ－１処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とを共用する。すなわち、ハッシュ値を算出するＳＨＡ－１処理においては、高速に動作する加算器が設けられた演算処理コア回路が必要とされる。また、楕円曲線暗号化処理においても、演算処理コア回路に加算器が設けられる。そこで、暗号化装置においては、ＳＨＡ－１処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とにおける加算器等のゲート数が多いハードウェア構成要素を共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【００３１】

さらに、暗号化装置においては、暗号化エンジンにおけるバス切り替えスイッチ群とその他各種機能の切り替えスイッチとを共用する。すなわち、公開鍵暗号化方式における鍵長を可変とするためにはバスを切り替える必要があることから、楕円曲線暗号化処理を行う暗号化エンジンには、例えば３２ビット幅のスイッチが多数設けられる。これらのスイッチは、その構成上、ＳＨＡ－１処理やＤＥＳ暗号化処理を行うハードウェアにおいても共用可能である。そこで、暗号化装置においては、これらバス切り替えスイッチ群を、その他各種機能の切り替えスイッチとして流用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【００３２】

さらにまた、暗号化装置においては、レジスタやメモリ等のハードウェアを時分割共用する。すなわち、暗号化装置における公開鍵暗号化方式の信号処理は、

ＤＥＳ暗号化処理を用いた乱数の生成、ＳＨＡ－１処理によるハッシュ値の算出、及び楕円曲線暗号化処理における楕円曲線の算出に大別される。しかしながら、これらの処理は、同時には行うことができないものであることから、ハードウェアを共用する場合には必然的に時分割処理を行うことになる。そこで、暗号化装置においては、これを利用して、レジスタやメモリ等のハードウェアを各処理で時分割共用する。これにより、暗号化装置は、回路規模の削減と電力消費の削減とを図ることが可能となる。

【００３３】

このように、暗号化装置は、楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理を行うための各ハードウェアを共用し、時分割処理を行うものとして構成される。

【００３４】

さて、暗号化装置においては、具体的に実装するにあたって、各ハードウェアを共用するために、楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理を行うための各ハードウェアを共用しやすい構成にする必要がある。以下では、これらの楕円曲線暗号化処理、ＳＨＡ－１処理、及びＤＥＳ暗号化処理を行うための各ハードウェアを共用しやすい構成とした具体的な実装例について説明した後、これらの各ハードウェアを統合した具体的な暗号化装置の実装例について説明する。

【００３５】

まず、ＳＨＡ－１処理を行うためのハードウェアであるＳＨＡ－１処理回路について説明する。

【００３６】

ＳＨＡ－１処理回路は、ＳＨＡ－１処理を行うものである。ＳＨＡ－１とは、認証やディジタル署名等に用いられるハッシュ関数の１つであり、５１２ビットの任意の原文から１６０ビットの擬似乱数であるハッシュ値を発生する不可逆な一方向性関数である。ＳＨＡ－１は、原文が１ビットでも異なる場合には、全く異なるハッシュ値を出力することから、ハッシュ値を生成して通信経路の両端で比較することにより、通信途中で原文が改竄されたか否かを検出する用途に広く

用いられる。具体的には、ＳＨＡ－１を用いたＳＨＡ－１処理においては、あるメッセージを送信する場合には、送信側がメッセージとこのメッセージに対するハッシュ値とを同時に送信し、受信側では受け取ったメッセージからハッシュ値を算出し、その結果得られたハッシュ値と送信側から送信されたハッシュ値とを比較することにより、データの改竄の有無を検証することができる。ＳＨＡ－１処理回路は、このようなＳＨＡ－１処理を行うものとして構成されるが、ここでは、いわゆるＦＩＰＳ（Federal Information Processing Standard）に規定されているＳＨＡ－１のうち、回路規模が比較的小さくて済む”ALTERNATIVE METHOD”を採用する。

【００３７】

この”ALTERNATIVE METHOD”のアルゴリズムは、通常であれば８０個の３２ビット・ワード配列Ｗ（０），・・・，Ｗ（７９）を用いて行うＳＨＡ－１処理を少ないメモリ空間で実現するための代替手段であり、｛Ｗ（ｔ）｝を循環キューとみなし、１６個の３２ビット・ワード配列Ｗ（０），・・・，Ｗ（１５）を用いて行うものである。このアルゴリズムにおいては、５１２ビット長のブロックＭ（ｉ）毎に、以下の４つの工程が行われる。なお、以下における値ＭＡＳＫは、１６進数で００００００００Ｆとする。

【００３８】

まず、このアルゴリズムにおいては、第１の工程として、ブロックＭ（ｉ）を１６個のワードＷ（０），・・・，Ｗ（１５）に分割する。なお、ワードＷ（０）は、最も左側のワードである。

【００３９】

続いて、このアルゴリズムにおいては、はじめの５つのワードバッファを、それぞれ、Ａ，Ｂ，Ｃ，Ｄ，Ｅとし、次の５つのワードバッファを、それぞれ、Ｈ０，Ｈ１，Ｈ２，Ｈ３，Ｈ４とすると、第２の工程として、次式（１）に示す演算を行う。

【００４０】

【数１】

$$\begin{cases} A = H0; \\ B = H1; \\ C = H2; \\ D = H3; \\ E = H4; \end{cases} \quad \cdots(1)$$

【００４１】

続いて、このアルゴリズムにおいては、第３の工程として、変数ｔを”０”から”７９”まで変化させ、次式（２）に示す演算を行う。

【００４２】

【数２】

$$\begin{cases} s = t \ AND \ MASK; \\ if\,(t \geq 16) \\ \quad W[s] = S1(W[(s+13) \ AND \ MASK] \ XOR \ W[(s+8) \ AND \ MASK] \\ \qquad\qquad XOR \ W[(s+2) \ AND \ MASK] \ XOR \ W[s]); \\ TEMP = S5(A) + F(t;B,C,D) + E + W[s] + Kt; \\ E = D; \\ D = C; \\ C = S30(B); \\ B = A; \\ A = TEMP; \end{cases} \quad \cdots(2)$$

【００４３】

なお、上式（２）におけるＳｎ（Ｘ）は、Ｘをワード値、ｎを０≦ｎ＜３２の整数としたときの循環左シフト操作を表すものである。また、上式（２）におけるＦ（ｔ；Ｂ，Ｃ，Ｄ）は、次式（３）に示す関数であり、Ｋ（ｔ）は、次式（４）に示す１６進数のワード定数列である。

【００４４】

【数３】

$$\begin{cases} F(t;B,C,D) = (B\ AND\ C)OR((NOT\ B)AND\ D) & (0 \le t \le 19) \\ F(t;B,C,D) = B\ XOR\ C\ XOR\ D & (20 \le t \le 39) \\ F(t;B,C,D) = (B\ AND\ C)OR(B\ AND\ D)OR(C\ AND\ D) & (40 \le t \le 59) \\ F(t;B,C,D) = B\ XOR\ C\ XOR\ D & (60 \le t \le 79) \end{cases} \quad \cdots(3)$$

【００４５】

【数４】

$$\begin{cases} K(t) = 5A827999 & (0 \le t \le 19) \\ K(t) = 6ED9EBA1 & (20 \le t \le 39) \\ K(t) = 8F1BBCDC & (40 \le t \le 59) \\ K(t) = CA62C1D6 & (60 \le t \le 79) \end{cases} \quad \cdots(4)$$

【００４６】

そして、このアルゴリズムにおいては、第４の工程として、次式（５）に示す演算を行い、一連の処理を終了する。

【００４７】

【数５】

$$\begin{cases} H0 = H0 + A; \\ H1 = H1 + B; \\ H2 = H2 + C; \\ H3 = H3 + D; \\ H4 = H4 + E; \end{cases} \quad \cdots(5)$$

【００４８】

ここで、このような"ALTERNATIVE METHOD"のアルゴリズムを一般的な形式で実

装すると、ＳＨＡ－１処理回路は、図２に示すような構成となる。

【００４９】

すなわち、ＳＨＡ－１処理回路は、同図に示すように、図示しないＣＰＵ（Central Processing Unit）から供給される演算用の値をテンポラリに保持するシフトレジスタ群１０と、上述したワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅとしての５つのシフトレジスタと上述した値ＴＥＭＰを保持するシフトレジスタとからなり結果としてのハッシュ値を取り込むためのシフトレジスタ群２０と、初期値Ｈ０，Ｈ１，Ｈ２，Ｈ３，Ｈ４及び上式（４）に示した１６進数のワード定数列Ｋ（ｔ）を保持するＲＯＭ（Read Only Memory）３０と、結果としてのハッシュ値を格納するＡＬＵ　ＲＡＭ（Arithmetic and Logical Unit Random Access Memory）４０とを備えるとともに、上述したアルゴリズムにおける各種演算を行うための各種演算処理回路を備える。なお、同図におけるＭＵＸ０，ＭＵＸ３，ＭＵＸ４，ＭＵＸ５は、それぞれ、バス切り替えスイッチである。

【００５０】

ここで、ＳＨＡ－１処理回路においては、回路規模を考慮すると、上式（２）中、値ＴＥＭＰの算出式、すなわち、次式（６）に示す演算を実行する３２ビット５入力の加算器が最も回路規模の増大を招来する要因となる。そこで、ＳＨＡ－１処理回路としては、楕円曲線暗号化処理の演算時間に比べてＳＨＡ－１処理の演算時間が無視できるほど短いことを利用して、図３に示すように、３２ビット２入力の加算器を４回用いることにより、回路規模を削減することが可能となる。

【００５１】

【数６】

$$TEMP = S5(A) + F(t;B,C,D) + E + W[s] + Kt; \qquad \cdots(6)$$

【００５２】

この場合、ＳＨＡ－１処理回路においては、図２に示した構成の場合に比べ、演算時間が約４～５倍程度になるものの、楕円曲線暗号化処理の演算時間に比べれば十分短時間であることから、実用上は何らの支障も招来せず、サイズが膨大

なデータやストリームに対してＳＨＡ－１処理を施すような特殊な場合を除けば、十分な性能を得ることが可能である。

【００５３】

なお、ＳＨＡ－１処理回路においては、後述するように、楕円曲線暗号化処理の際に使用する加算器と兼用することにより、当該ＳＨＡ－１処理回路における加算器そのものが不要となることから、さらに大幅な回路規模の削減を図ることが可能となる。

【００５４】

また、ＳＨＡ－１処理回路においては、上式（２）中、ワードＷ［ｓ］の算出式、すなわち、次式（７）に示す演算を実行する際に、必ず３２ビット×１６段のシフトレジスタが必要となることがわかる。

【００５５】

【数７】

$$W[s]=S1(W[(s+13)\ AND\ MASK]\ XOR\ W[(s+8)\ AND\ MASK]\ XOR\ W[(s+2)\ AND\ MASK]\ XOR\ W[s]);\quad \cdots(7)$$

【００５６】

さらに、ＳＨＡ－１処理回路においては、上式（２）中、ワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅの算出式、すなわち、次式（８）に示す演算を実行する際にも、少なくとも３２ビット×５～６段のシフトレジスタが必要となる。

【００５７】

【数８】

$$\begin{cases} E=D; \\ D=C; \\ C=S30(B); \\ B=A; \\ A=TEMP; \end{cases} \quad \cdots(8)$$

【００５８】

ここで、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化

処理回路においては、後述するように、段数が可変とされる３２ビット×７段のシフトレジスタ群が３組設けられることから、ＳＨＡ－１処理回路においては、これらのシフトレジスタを流用することにより、当該ＳＨＡ－１処理回路に専用のシフトレジスタを設ける必要がなくなり、さらに大幅な回路規模の削減を図ることが可能となる。結果的に、暗号化装置においては、通常であれば６００００ゲート以上からなるＳＨＡ－１処理回路を、楕円曲線暗号化処理回路に対して２０００ゲート程度の追加回路のみで実現することができる。

【００５９】

さて、このようなＳＨＡ－１処理回路は、図４及び図５に示すような一連の工程を経ることにより、基本動作を行う。なお、ここでは、先に図２に示した構成からなるＳＨＡ－１処理回路の基本動作について説明する。

【００６０】

まず、ＳＨＡ－１処理回路は、図４に示すように、ステップＳ１において、変数ｔを”０”とする。

【００６１】

続いて、ＳＨＡ－１処理回路は、ステップＳ２において、シフトレジスタ群１０における各シフトレジスタに対して、パディングされたデータのうち、３２×１６ブロック（＝５１２ビット）からなる先頭のデータをロードする。

【００６２】

続いて、ＳＨＡ－１処理回路は、ステップＳ３において、バス切り替えスイッチＭＵＸ０を、演算処理回路Ｗ［ｓ］の出力側に切り替える。

【００６３】

続いて、ＳＨＡ－１処理回路は、ステップＳ４において、初期値Ｈ０，Ｈ１，Ｈ２，Ｈ３，Ｈ４をＲＯＭ３０から読み出し、バス切り替えスイッチＭＵＸ４、加算器、及びシフトレジスタ群２０における値ＴＥＭＰを保持するシフトレジスタを介して、シフトレジスタ群２０におけるワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅとしての各シフトレジスタに対して順次ロードする。

【００６４】

続いて、ＳＨＡ－１処理回路は、ステップＳ５において、値ＴＥＭＰとしてオ

ールゼロをセットする。

【００６５】

続いて、ＳＨＡ－１処理回路は、ステップＳ６において、バス切り替えスイッチＭＵＸ５を制御して、次式（９）に示すように、加算器によって４回に分けた加算処理を行うことにより、上式（６）に示した演算と等価な演算を行い、値ＴＥＭＰを算出する。

【００６６】

【数９】

$$\begin{cases} S5(A)+F(t)\Rightarrow TEMP; \\ TEMP+E\Rightarrow TEMP; \\ TEMP+W[s]\Rightarrow TEMP; \\ TEMP+K(t)\Rightarrow TEMP; \end{cases} \quad \cdots(9)$$

【００６７】

続いて、ＳＨＡ－１処理回路は、ステップＳ７において、バス切り替えスイッチＭＵＸ３を、演算処理回路Ｓ３０の出力側に切り替え、各シフトレジスタに保持されている値ＴＥＭＰ，Ａ．Ｂ．Ｃ．Ｄ．Ｅを、それぞれ、１クロック分だけ右にシフトする。これにより、ＳＨＡ－１処理回路は、上式（８）に示した各値を得ることができる。

【００６８】

続いて、ＳＨＡ－１処理回路は、ステップＳ８において、シフトレジスタ群１０における各シフトレジスタに保持されている値を、それぞれ、１クロック分だけ右にシフトする。

【００６９】

続いて、ＳＨＡ－１処理回路は、ステップＳ９において、変数ｔが”７９”に到達したか否かを判定する。ここで、ＳＨＡ－１処理回路は、変数ｔが”７９”に到達していないものと判定した場合には、ステップＳ１０へと処理を移行し、変数とを”１”だけインクリメントした後、ステップＳ２乃至ステップＳ８の処理を繰り返す。すなわち、ＳＨＡ－１処理回路は、ステップＳ２乃至ステップＳ８の処理を、変数ｔを”０”から”７９”まで変化させて行う。

【００７０】

一方、ＳＨＡ－１処理回路は、変数ｔが”７９”に到達したものと判定した場合には、ステップＳ１１へと処理を移行し、バス切り替えスイッチＭＵＸ３を、演算処理回路Ｓ３０の出力側とは反対側に切り替えるとともに、バス切り替えスイッチＭＵＸ４を、ＲＯＭ３０の出力側に切り替え、さらに、バス切り替えスイッチＭＵＸ５の出力をワードバッファＥとしてのシフトレジスタからの出力とすることにより、ワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅとしての各シフトレジスタに保持されている値に対して、それぞれ、初期値Ｈ０，Ｈ１，Ｈ２，Ｈ３，Ｈ４を加算器によって加算する。

【００７１】

続いて、ＳＨＡ－１処理回路は、ステップＳ１１における加算器による演算結果が、値ＴＥＭＰを保持するシフトレジスタに供給されることから、ステップＳ１２において、上式（５）の演算を実現するように、各シフトレジスタに保持されている値を、それぞれ、６クロック分だけ右にシフトする。

【００７２】

そして、ＳＨＡ－１処理回路は、図５に示すように、ステップＳ１３において、ワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅとしての各シフトレジスタに保持されている値を、それぞれ、ＡＬＵ　ＲＡＭ４０に格納する。

【００７３】

続いて、ＳＨＡ－１処理回路は、ステップＳ１４において、パディングの結果が５１２ビットであるか否かを判定する。

【００７４】

ここで、ＳＨＡ－１処理回路は、パディングの結果が５１２ビットであるものと判定した場合には、ステップＳ１３においてＡＬＵ　ＲＡＭ４０に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

【００７５】

一方、ＳＨＡ－１処理回路は、パディングの結果が５１２ビットでない、すなわち、５１２ビットを超えるものと判定した場合には、ステップＳ１５において、パディングしたデータが全てシフトレジスタ群１０における各シフトレジスタ

に対してロードされて処理が終了したか否かを判定する。

【００７６】

ここで、ＳＨＡ－１処理回路は、パディングしたデータが全てシフトレジスタ群１０における各シフトレジスタに対してロードされておらず処理が終了していないものと判定した場合には、ステップＳ１６において、ステップＳ１３における状態を保持しつつ、次の５１２ビットのデータをシフトレジスタ群１０における各シフトレジスタに対してロードする。

【００７７】

続いて、ＳＨＡ－１処理回路は、ステップＳ１７において、バス切り替えスイッチＭＵＸ４を、ＡＬＵ　ＲＡＭ４０の出力側に切り替え、ステップＳ１３においてＡＬＵ　ＲＡＭ４０に格納された値を、それぞれ、ワードバッファＡ，Ｂ，Ｃ，Ｄ，Ｅとしての各シフトレジスタに対してロードする。

【００７８】

続いて、ＳＨＡ－１処理回路は、ステップＳ１８において、バス切り替えスイッチＭＵＸ０を、演算処理回路Ｗ［ｓ］の出力側に切り替え、図４中ステップＳ５からの処理を繰り返す。

【００７９】

そして、ＳＨＡ－１処理回路は、ステップＳ１５における判定の結果、パディングしたデータが全てシフトレジスタ群１０における各シフトレジスタに対してロードされて処理が終了したものと判定した場合には、ステップＳ１３においてＡＬＵ　ＲＡＭ４０に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

【００８０】

ＳＨＡ－１処理回路は、このような一連の処理を行うことにより、ハッシュ値を生成する。

【００８１】

つぎに、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化処理回路について説明する。

【００８２】

楕円曲線暗号化処理回路は、楕円曲線暗号化処理を行うものである。楕円曲線暗号化とは、暗号化と復号とに異なる通信鍵を用いる公開鍵暗号化アルゴリズムの１つであり、１６０ビット長の鍵を用いることにより、１０２４ビット長の鍵を用いたいわゆるＲＳＡ（Rivest-Shamir-Adleman）暗号化方式と同等の性能を発揮する暗号化方式である。暗号化装置において、楕円曲線暗号化処理回路は、いわゆるモンゴメリー（Montgomery）法を用いて構成される。すなわち、楕円曲線暗号化処理回路は、図６に示すように、図示しないＣＰＵから供給される演算用の値をテンポラリに保持する３２ビット幅のシフトレジスタ群５０，６０と、結果を取り込むためのシフトレジスタ群７０と、主に３２ビット幅の入力を有する図示しない加算器、減算器、及び乗算器を内部に有する楕円曲線演算処理コア回路８０とを備える。なお、同図におけるＭＵＸ０，ＭＵＸ１，ＭＵＸ２は、それぞれ、バス切り替えスイッチである。

【００８３】

このような楕円曲線暗号化処理回路においては、モンゴメリー法と称される特殊な手法を用いて処理の高速化及び回路規模の削減を実現する。モンゴメリー法による楕円曲線演算処理コア回路８０は、主に、加算器、減算器、及び乗算器の組み合わせ回路によって構成され、演算のステップ毎に３２ビット幅のデータ同士の処理を行う。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線演算処理コア回路８０の内部に設けられる加算器を、ＳＨＡ－１処理回路における加算器と共用する。

【００８４】

さらに、モンゴメリー法による楕円曲線演算処理コア回路８０と、これと共用されるＳＨＡ－１処理回路を構成する乗算器による処理においては、加算器及び減算器が処理に要する処理時間に比べて乗算器が処理に要する処理時間は大きい。従って、これに伴う処理の遅延は、ゲートにおいて消費される消費電力が鋭いピークを持つことを抑制し、ゲートにおける瞬時電力を低減することが可能となる。

【００８５】

また、楕円曲線暗号化処理回路においては、３組の３２ビット幅のシフトレジ

スタ群５０，６０，７０が設けられるが、例えば１６０ビット幅、１９２ビット幅、又は２２４ビット幅にも対応するために、各シフトレジスタ群５０，６０，７０のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチＭＵＸ０，ＭＵＸ１，ＭＵＸ２が設けられる。すなわち、楕円曲線暗号化処理回路においては、１６０ビット幅、１９２ビット幅、又は２２４ビット幅にも対応するために、３組の３２ビット幅のシフトレジスタ群５０，６０，７０が、それぞれ、５，６，７段に切り替え可能に構成される。

【００８６】

この具体例としては、図７（Ａ）にシフトレジスタ群６０の近傍の要部構成を示すように、入力と、５段目、６段目、及び７段目のシフトレジスタのそれぞれからの出力とのうち、いずれか１つの信号を、バス切り替えスイッチＭＵＸ１からの出力とするように、シフトレジスタ群６０における各シフトレジスタのうち、右側のシフトレジスタから個数を可変とするものが考えられる。また、他の具体例としては、図７（Ｂ）にシフトレジスタ群６０の近傍の要部構成を示すように、入力と、７段目のシフトレジスタのそれぞれからの出力とのうち、いずれか１つの信号を出力とするバス切り替えスイッチＭＵＸ１を設けるとともに、１段目のシフトレジスタの後段にバス切り替えスイッチＭＵＸ２を設け、さらに、２段目のシフトレジスタの後段にバス切り替えスイッチＭＵＸ３を設けるといったように、シフトレジスタ群６０における各シフトレジスタのうち、左側のシフトレジスタから個数を可変とするものが考えられる。なお、楕円曲線暗号化処理回路においては、シフトレジスタ群５０，７０についても、同様に構成することができる。

【００８７】

このように、楕円曲線暗号化処理回路においては、３組の３２ビット幅のシフトレジスタ群５０，６０，７０のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチＭＵＸ０，ＭＵＸ１，ＭＵＸ２が設けられる。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線暗号化処理回路におけるシフトレジスタ群５０，６０，７０と、ＳＨＡ－１処理回路におけるシフトレジスタとを共用するとともに、楕円曲線暗号化処理回

路におけるバス切り替えスイッチＭＵＸ０，ＭＵＸ１，ＭＵＸ２と、ＳＨＡ－１処理回路におけるバス切り替えスイッチとを共用する。

【００８８】

さらに、上述したＳＨＡ－１処理回路は、先に図３に示したように構成すると、３２ビット幅のシフトレジスタ群を用いて構成することができる。このようなＳＨＡ－１処理回路において、最終的な結果としてのハッシュ値や演算途中経過の値を保持するシフトレジスタは、先に図２に示したように、ＡＬＵ　ＲＡＭに代替することができる。したがって、暗号化装置においては、楕円曲線暗号化処理回路における演算処理で用いる図示しないＡＬＵ　ＲＡＭとＳＨＡ－１処理回路におけるＡＬＵ　ＲＡＭとを共用する。これにより、暗号化装置においては、回路規模を抑制するのみならず、次回の楕円曲線暗号化処理にて用いるハッシュ値をＡＬＵ　ＲＡＭに即座に格納することから、データ転送の手間を省略し、処理の高速化を図ることも可能となる。

【００８９】

また、楕円曲線暗号化処理回路にて算出された値や、ＳＨＡ－１処理回路における最終的な結果としてのハッシュ値や演算途中の値をＡＬＵ　ＲＡＭに格納するために、楕円曲線暗号化処理回路やＳＨＡ－１処理回路がＡＬＵ　ＲＡＭにアクセスするに際しては、消費される電力が当該暗号化処理回路における他の各種信号処理において消費される電力のピークに比べてその電力のピークが大きい。そこで、後述するように、楕円曲線暗号化処理回路やＳＨＡ－１処理回路がＣＰＵやＲＡＭからデータを受け取るに際してのゲートを制御し、ＡＬＵ　ＲＡＭへのアクセス以外の各種処理を制限することにより、ＡＬＵ　ＲＡＭへのアクセスと、他の各種処理とを時分割にて行い、該暗号化処理回路にて消費される消費電力のピークを低減することが可能となる。

【００９０】

また、楕円曲線暗号化処理回路やＳＨＡ－１処理回路へのゲートが制限されるに際して、これら処理回路がＣＰＵからの指示に関するデータを受け取ることなく処理を行うために、これら処理回路は自立的に処理を行うことができる。従って、該暗号化処理装置全体における瞬時電力を低減することができ、瞬時電力が

制限電力を超えた場合における再処理動作を行うことを低減することができ、処理を高速に行うことが可能となる。

【００９１】

最後に、ＤＥＳ暗号化処理を行うためのハードウェアであるＤＥＳ暗号化処理回路について説明する。

【００９２】

ＤＥＳ暗号化処理回路は、ＤＥＳ暗号化処理を行うものである。ＤＥＳ暗号化とは、暗号化と復号とに同じ通信鍵を用いる共通鍵暗号化アルゴリズムの１つである。暗号化装置において、ＤＥＳ暗号化処理回路は、ＤＥＳ暗号化処理を３重に行ういわゆるトリプルＤＥＳ暗号化処理を行うものとして構成される。

【００９３】

ここで、ＤＥＳ暗号化処理回路においては、トリプルＤＥＳ暗号化処理を行うことから、通常のシングルＤＥＳ暗号化処理を行う場合に比べ、鍵データを保持するシフトレジスタ群の規模が大きくなり、ビット列に対してＤＥＳ暗号化処理を施す際の連鎖技法であるいわゆるＣＢＣ（Cipher Block Chaining）モードを行う際にも、シフトレジスタ群が必要となる。したがって、ＤＥＳ暗号化処理回路においては、これらのシフトレジスタ群をゲート換算すると、いわゆるＳボックスに比較しても大きく、全体として回路規模を増大させる要因となる。

【００９４】

ところで、トリプルＤＥＳ暗号化処理は、１つのＤＥＳ演算処理コア回路を用いて、鍵データを３種類に変化させて３回演算処理を行うことによって実行される。そこで、ＤＥＳ暗号化処理回路としては、いわゆるＴｙｐｅ　Ａの非接触型ＩＣカードに適用する場合には、先に図６に示した楕円曲線暗号化処理回路におけるシフトレジスタ群７０を、この鍵データを保持するシフトレジスタ群として用いれば、楕円曲線暗号化処理回路に対する追加回路として、６４ビット幅又は３２ビット幅のバス切り替えスイッチを１つだけ設けるだけでよい。ここで、バス切り替えスイッチは、楕円曲線暗号化処理回路にも設けられていることから、ＤＥＳ暗号化処理回路としては、このバス切り替えスイッチを流用すれば追加回路も不要となる。一方、ＤＥＳ暗号化処理回路としては、いわゆるＴｙｐｅ　Ｂ

の非接触型ＩＣカードに適用する場合には、予め３種類の鍵データを用意しておき、シングルＤＥＳ暗号化処理を行う毎に、２個のシフトレジスタ分だけシフトして鍵データを交換することにより、Ｔｙｐｅ　Ａの場合と同様な動作を行うことができる。また、ＤＥＳ暗号化処理回路においては、データを保持するシフトレジスタや結果を保持するシフトレジスタについても、楕円曲線暗号化処理回路におけるシフトレジスタ群と共用することができることから、非常に僅かな追加回路でトリプルD.ＥＳ暗号化処理を行うことが可能となる。

【００９５】

このようなＤＥＳ暗号化処理回路は、具体的には、図８に示すように構成することができる。すなわち、ＤＥＳ暗号化処理回路は、図示しないＣＰＵから供給されるデータを保持する３２ビット幅のシフトレジスタ群９０と、鍵データを保持するシフトレジスタ群１００と、ＤＥＳ演算処理コア回路１２０を有する演算処理回路１１０とを備える。なお、同図におけるＭＵＸ，ＭＵＸ０は、それぞれ、バス切り替えスイッチである。

【００９６】

ＤＥＳ暗号化処理回路においては、本来であれば６４ビット幅のバッファを必要とするところ、３２ビット幅のシフトレジスタ群９０，１００でまかなうことができる。また、ＤＥＳ暗号化処理回路においては、トリプルＤＥＳ暗号化処理に用いる鍵データの交換を行うためにバス切り替えスイッチを用いず、巡回させる形式とすることにより、バス切り替えスイッチを不要としている。このように、ＤＥＳ暗号化処理回路は、上述した楕円曲線暗号化処理回路に対して、ＤＥＳ演算処理コア回路１２０を含む演算処理回路１１０以外には殆ど追加回路を必要とせず、大幅に回路規模を削減することが可能となる。

【００９７】

さて、以上では、各部を共用しやすい構成としたＳＨＡ－１処理回路、楕円曲線暗号化処理回路、及びＤＥＳ暗号化処理回路について説明したが、以下では、これらのＳＨＡ－１処理回路、楕円曲線暗号化処理回路、及びＤＥＳ暗号化処理回路を統合して暗号化装置を構成することを考える。

【００９８】

先に図２に示したＳＨＡ－１処理回路、図６に示した楕円曲線暗号化処理回路、及び図８に示したＤＥＳ暗号化処理回路を、それぞれ、重ね合わせると、共通の構成部位が極めて多く存在することがわかる。したがって、暗号化装置は、図９に示すように構成することができる。

【００９９】

すなわち、暗号化装置は、同図に示すように、２つのシフトレジスタ群２００，２１０と、先に図２に示したＳＨＡ－１処理回路におけるＲＯＭ３０に相当するＲＯＭ２２０と、先に図２に示したＳＨＡ－１処理回路におけるＡＬＵ　ＲＡＭ４０及び先に図６に示した楕円曲線暗号化処理回路における楕円曲線演算処理コア回路８０として機能するモンゴメリー演算回路２３０と、先に図８に示したＤＥＳ暗号化処理回路における演算処理回路１１０に相当する演算処理回路２４０と、ＳＨＡ－１処理における各種演算を行うための上述した各種演算処理回路とを備える。なお、同図においては、シフトレジスタ群２００と演算処理回路２４０との配線については図示を省略している。

【０１００】

より具体的には、暗号化装置においては、先に図２に示したＳＨＡ－１処理回路におけるシフトレジスタ群１０と、先に図６に示した楕円曲線暗号化処理回路におけるシフトレジスタ群５０，６０と、先に図８に示したＤＥＳ暗号化処理回路におけるシフトレジスタ群９０，１００とを、シフトレジスタ群２００として共用する。また、暗号化装置においては、先に図２に示したＳＨＡ－１処理回路におけるシフトレジスタ群２０と、先に図６に示した楕円曲線暗号化処理回路におけるシフトレジスタ群７０とを、シフトレジスタ群２１０として共用する。

【０１０１】

さらに、暗号化装置においては、モンゴメリー演算回路２３０とＳＨＡ－１処理にて用いられる加算器とを、バス切り替えスイッチＭＵＸを介して接続することにより、楕円曲線暗号化処理にて用いられる加算器を削減している。

【０１０２】

さらにまた、暗号化装置においては、先に図２に示したＳＨＡ－１処理回路におけるバス切り替えスイッチＭＵＸ０と、先に図６に示した楕円曲線暗号化処理

回路におけるバス切り替えスイッチＭＵＸ０と、先に図８に示したＤＥＳ暗号化処理回路におけるバス切り替えスイッチＭＵＸ０とを共用するとともに、先に図６に示した楕円曲線暗号化処理回路におけるバス切り替えスイッチＭＵＸ１と、先に図８に示したＤＥＳ暗号化処理回路におけるバス切り替えスイッチＭＵＸ０とを共用する。

【０１０３】

このように、暗号化装置においては、ＳＨＡ－１処理回路、楕円曲線暗号化処理回路、及びＤＥＳ暗号化処理回路における各部を共用することができ、後述する各処理モードに応じて動作させるハードウェアを時分割に切り替えることにより、本来必要とされるゲート数の約１／２程度のゲート数にまで回路規模を削減することができる。また、暗号化装置においては、回路規模の削減にともない、消費電力も約１／２程度にまで削減することができる。

【０１０４】

さらに、後述するＡＬＵ　ＲＡＭへのアクセスが行われるに際して、他の各種処理を制限することにより該暗号化処理装置全体で消費される電力の瞬時電力を低減することができる。特に、楕円暗号化処理回路やＳＨＡ－１処理回路にて演算された結果である値やハッシュ値を格納するＡＬＵ　ＲＡＭへアクセスするに際しては、他の各種処理に比べて消費される瞬時電力が大きいことから、各種処理モードに応じて動作させるハードウェアを時分割で動作させることにより瞬時電力のピークを低減し、瞬時電力が制限電力を超えることによる再処理動作を行うことなく、高速な処理を可能とする。

【０１０５】

さらに、暗号化装置においては、これらの各部を制御する図示しないＣＰＵの負荷も削減することができる。例えば、暗号化装置においては、ＳＨＡ－１処理によって算出されたハッシュ値のＡＬＵ　ＲＡＭ上における格納場所を、楕円曲線暗号化処理にて用いられるアドレスに予め設定しておくことにより、ＳＨＡ－１処理によるハッシュ値の算出後に、そのまま楕円曲線暗号化処理へと即座に移行することができることから、署名生成及び署名検証等の一連の動作の大半をハードウェアによって高速に実行することができる。したがって、暗号化装置にお

いては、ＣＰＵの負荷を削減することができ、さらには、ソフトウェアの改竄等による攻撃に対する耐性も強固となる。通常、暗号化処理においては、途中の演算結果の授受をＣＰＵに委任した場合には、ソフトウェアを改竄することによって容易に成りすましを許容してしまう一方で、暗号化装置においては、このような演算途中におけるＣＰＵの介入による改竄を回避することができる。

【０１０６】

さて、以下では、このような暗号化装置を適用した応用例について説明する。

【０１０７】

暗号化装置は、上述したように、非接触型ＩＣカードに適用することができる。

【０１０８】

非接触ＩＣカードは、例えば図１０に示すように、各部を制御するＣＰＵ３００と、このＣＰＵ３００のワークエリアとして機能するメモリであって例えば２ＫＢ程度の容量を有するＲＡＭ３１０と、各種プログラム等を記憶する読み出し専用のメモリであって例えば３２ＫＢ程度の容量を有するＲＯＭ３２０と、電気的に書き換え可能とされるメモリであって例えば９ＫＢ程度の容量を有するＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）３３０と、電源回路等のアナログブロック３４０と、無線通信を行うためのＲＦ（Radio Frequency）ブロック３５０と、上述した楕円曲線暗号化処理、ＳＨＡ－１処理、及びトリプルＤＥＳ暗号化処理を行う暗号化装置に相当するＥＣＣ／ＳＨＡ１／ＤＥＳブロック３６０と、例えば１ＫＢ程度の容量を有する上述したＡＬＵＲＡＭ３７０と、テスター用のランドからなるテストブロック３８０と、ＣＰＵ３００と各部との間でデータの授受を行うためのバスであるＣＰＵインターフェース３９０とを集積回路化したいわゆるＬＳＩ（Large Scale Integration）として構成される。

【０１０９】

このような非接触型ＩＣカードは、先に図９に示した暗号化装置がＥＣＣ／ＳＨＡ１／ＤＥＳブロック３６０として組み込まれたものである。非接触ＩＣカードは、ＣＰＵ３００の制御のもとに、ＥＣＣ／ＳＨＡ１／ＤＥＳブロック３６０

を動作させ、楕円曲線暗号化処理、ＳＨＡ－１処理、及びトリプルＤＥＳ暗号化処理を行う。このとき、非接触型ＩＣカードは、上述したように、各処理モードに応じて、動作させるハードウェアを時分割に切り替える。

【０１１０】

この時分割動作を具体的に説明するために、図１１に示すように、各部を機能的に表現する。なお、同図においては、アナログブロック３４０については図示を省略するとともに、説明の便宜上、ＥＣＣ／ＳＨＡ１／ＤＥＳブロック３６０を、楕円曲線暗号化処理及びＳＨＡ－１処理の機能を表すＥＣＣ／ＳＨＡ１ブロック３６０$_1$と、トリプルＤＥＳ暗号化処理の機能を表すＤＥＳブロック３６０$_2$とに大別して表現している。

【０１１１】

このような非接触型ＩＣカードにおける処理モードは、主に、通信を行う通信モード、楕円曲線暗号化処理を行う楕円曲線暗号化処理モード、トリプルＤＥＳ暗号化処理を行うＤＥＳ暗号化処理モード、及びＡＬＵ　ＲＡＭ３７０に対してアクセスするＡＬＵ　ＲＡＭモードの４つに大別される。

【０１１２】

非接触型ＩＣカードにおいては、通信モード時には、図１２（Ａ）中太線枠で示すように、ＣＰＵ３００、ＲＡＭ３１０、ＲＯＭ３２０、ＥＥＰＲＯＭ３３０、及びＲＦブロック３５０が動作する。すなわち、非接触型ＩＣカードにおいては、通信モード時には、ＣＰＵ３００の制御のもとに、ＲＯＭ３２０に記憶されている所定の通信プログラムが起動し、ＲＡＭ３２０やＥＥＰＲＯＭ３３０に記憶されている各種情報が、ＲＦブロック３５０を介して外部に送信されるとともに、ＲＦブロック３５０を介して外部から受信した各種情報が、ＲＡＭ３２０やＥＥＰＲＯＭ３３０に記憶される。また、通信モード時には、暗号エンジンは各種処理を行うことがなく、該非接触型ＩＣカード全体における消費電力は、通信モードで消費される電力に略等しくなる。つまり、通信モード、楕円曲線暗号化処理モード、トリプルＤＥＳ暗号化処理モード、及びＡＬＵ　ＲＡＭモードを同時刻に動作させて各種処理を行うことがなく、通信モード時に消費される該非接触型ＩＣカード全体における消費電力は、通信モードを動作させるに際して消費

される電力のみによって決まる。従って、該非接触型ＩＣカードにおける消費電力を低減することができるだけでなく、各モードを動作させるに際して消費される電力が同一時刻で加算される結果、該非接触型ＩＣカード全体における瞬時電力が制限電力を超えないように各種処理を行うことが可能となる。

【０１１３】

また、非接触型ＩＣカードにおいては、楕円曲線暗号化処理モード時には、同図（Ｂ）中太線枠で示すように、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$が動作する。すなわち、非接触型ＩＣカードにおいては、楕円曲線暗号化処理モード時には、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$によってＳＨＡ－１処理が行われ、ハッシュ値を生成する。また、楕円曲線暗号化処理モード時には、ＣＰＵ３００、ＲＡＭ３１０、ＲＯＭ３２０、ＥＥＰＲＯＭ３３０、及びＲＦブロック３５０がアイドリング状態とされ、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$からＡＬＵ　ＲＡＭ３７０へのハッシュ値の格納又はＡＬＵ　ＲＡＭ３７０からのハッシュ値の読み込みが制限される。

【０１１４】

また、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$は、楕円曲線暗号化処理モード時にＣＰＵ３００から送られる処理に関する命令の如きアシストを受けることなく、自立的に処理を行うことができ、ＣＰＵ３００、ＲＡＭ３１０、ＲＯＭ３２０、ＥＥＰＲＯＭ３３０、及びＲＦブロック３５０による各種処理に対して時分割にて行うことが可能となる。従って、個別の処理における消費電力を低減することが可能となる。ＥＣＣ／ＳＨＡ１ブロック３６０$_1$とＡＬＵ　ＲＡＭ３７０との間における演算結果としてのハッシュ値の格納又は読み込みに際しては、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$による演算処理中には、ＡＬＵ　ＲＡＭ３７０との間におけるハッシュ値の受け渡しを行うことがなく、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$の演算処理が一旦停止される。これにより、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$における演算処理と、ＡＬＵ　ＲＡＭ３７０へのアクセスが時分割で行われるように制限され、楕円曲線暗号化処理が行われる。

【０１１５】

さらに、非接触型ＩＣカードにおいては、ＤＥＳ暗号化処理モード時には、同

図（Ｃ）中太線枠で示すように、ＤＥＳブロック３６０$_2$が動作する。ここで、ＣＰＵ３００、ＲＡＭ３１０、ＲＯＭ３２０はアイドリング状態とされる。すなわち、非接触型ＩＣカードにおいては、ＤＥＳ暗号化処理モード時には、ＤＥＳブロック３６０$_2$が、ＣＰＵ３００の制御のもとに、ＲＯＭ３２０に記憶されている所定の擬似乱数（Pseudo-random Number；以下、ＰＮという。）系列がシード（seed）や鍵データとして読み出され、ＲＡＭ３１０がワークエリアとして用いられながら、ＤＥＳブロック３６０$_2$と、ＣＰＵ３００、ＲＯＭ３００及びＲＡＭ３１０が時分割にて動作し、トリプルＤＥＳ暗号化処理が行われる。

【０１１６】

さらに、非接触型ＩＣカードにおいては、ＡＬＵ　ＲＡＭモード時には、同図（Ｄ）中太線枠で示すように、ＡＬＵ　ＲＡＭ３７０が動作し、ＥＣＣ／ＳＨＡ１ブロックが生成する演算結果及びＡＬＵ　ＲＡＭ３７０に格納されたデータをＡＬＵ　ＲＡＭ３７０とＥＣＣ／ＳＨＡ１ブロック３６０$_1$との間で授受する。ＡＬＵ　ＲＡＭ３７０を動作させるに際しては、ＣＰＵ３００、ＲＡＭ３１０、ＲＯＭ３２０、ＥＥＰＲＯＭ３３０、及びＲＦブロック３５０がアイドリング状態とされ、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$とのデータの授受を制限し、消費電力を低減することができる。例えば、ＥＣＣ／ＳＨＡ１ブロック３６０$_1$を構成し、比較的消費電力が大きい乗算器から構成される回路にミュート回路を接続することにより、消費電力を低減することが可能となる。

【０１１７】

図１３は、縦軸を消費電力Ｗ、横軸を処理時刻Ｔとし、これら各処理モードにおいて消費される消費電力を比較した図である。同図（Ａ）はゲートにおける消費電力、同図（Ｂ）はＡＬＵ　ＲＡＭにおける消費電力、同図（Ｃ）はＲＡＭにおける消費電力、さらに同図（Ｄ）は、ＥＣＣ／ＳＨＡ１ブロックを構成するゲート、ＡＬＵ　ＲＡＭ、及びＲＡＭにける消費電力を加算した該非接触型ＩＣカードにおける全体の消費電力を示す。同図（Ａ）に示すように、ゲートにおける消費電力は、処理回路を構成する乗算器などの処理に際しての遅延によりピークが抑制されるとともに処理時間に沿って分散することになる。これにより、ゲートで消費される消費電力のみに関して瞬時電力が抑制されることになる。

【０１１８】

さらに、同図（Ａ）及び（Ｂ）に示すように、ＡＬＵ　ＲＡＭが処理回路にアクセスするに際してはゲートにおける処理が停止されることにより、ＡＬＵ　ＲＡＭで電力が消費されるタイミングにおいては、ゲートでは電力が消費されることがない。ＡＬＵ　ＲＡＭにおけて電力が消費される時刻t_0とゲートにおける電力が消費される時刻t_1とのタイミングがずれることにより、ゲートにおける消費電力とＡＬＵ　ＲＡＭにおける消費電力が同時に生じることがない。

【０１１９】

また、ＣＰＵやＲＡＭから自立的に処理を行うことができることにより、ＥＣＣ／ＳＨＡ１ブロックとＲＡＭとの間におけるデータの読み込みの回数を低減することができ、先に示した図１４（Ｃ）に比べ、図１３（Ｃ）に示すようにＲＡＭにおける消費電力を低減することもできる。

【０１２０】

従って、図１３（Ａ）乃至（Ｃ）に示す各処理における消費電力を加算し、非接触型ＩＣカードで消費される全体の消費電力は、同図（Ｄ）に示すように図１４（Ｄ）に示す消費電力に比べて瞬時電力が低減されたものとすることができ、例えば、非接触型ＩＣカードの制限電力が２０ｍＡである場合でも、制限電力を超えないように非接触型ＩＣカードを動作させることが可能となる。

【０１２１】

このように、非接触型ＩＣカードにおいては、比較的消費電力が大きい処理を行われるに際して、他の処理を制限することにより瞬時電力を低減することができ、制限電力を瞬時電力が超えることによる処理の遅延を生じることがなく高速な処理を行うことが可能となる。また、各処理モードに応じて、動作させるハードウェアを時分割に切り替えることにより、ハードウェアを共用した構成であっても、同時には行うことができない複数の処理を行うことが可能であるとともに、回路規模の削減と電力消費の削減とを図ることができる。

【０１２２】

以上説明したように、本発明の実施の形態として示す暗号化装置は、処理に際して瞬時電力が比較的大きいＡＬＵ　ＲＡＭへのアクセスに際して、他の各演算

処理を制限する。よって、他のＥＣＣ／ＳＨＡ１ブロックにおける処理のタイミングをずらすことにより瞬時電力を低減することができ、高速な処理を可能とすることができる。

【０１２３】

さらに、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を行うこともできる。

【０１２４】

したがって、暗号化装置は、ＬＳＩ等として実装する際に、チップサイズを大幅に小型化することができることから、非接触型ＩＣカード等にも容易に適用することができる。このとき、暗号化装置は、電力消費が少なくて済むことから、非接触型ＩＣカードに適用した場合であっても、数センチメートルもの実用的な通信距離を実現することができ、該非接触型ＩＣカードの動作時における消費電力が制限電力を超える度に再度処理をやり直すことなく、高速な処理を行うことが可能となる。また、暗号化装置は、改竄等の攻撃に対する耐性にも優れていることから、高い安全性が要求される非接触型ＩＣカードを用いたサービスに適用して有効である。

【０１２５】

なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、公開鍵暗号化方式として、楕円曲線暗号化方式を採用して説明したが、本発明は、例えばＲＳＡ暗号化方式等の他の公開鍵暗号化方式にも容易に適用することができる。

【０１２６】

また、上述した実施の形態では、ハッシュ関数として、ＳＨＡ－１を用いるものとして説明したが、本発明は、例えばＭＤ５（Message Digest 5）等の他のハッシュ関数にも容易に適用することができる。

【０１２７】

さらに、上述した実施の形態では、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の１つであるＤＥＳ暗号化方式

を用いて生成するものとして説明したが、本発明は、乱数生成の手法については、任意のものを適用することができる。

【０１２８】

さらにまた、上述した実施の形態では、暗号化装置の適用例として、非接触型ＩＣカードを用いて説明したが、本発明は、同様の機能を要求する任意の装置やデバイスに適用することができるのは勿論である。

【０１２９】

このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【０１３０】

【発明の効果】

以上詳細に説明したように、本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限する。

【０１３１】

したがって、本発明にかかる暗号化装置は、ハッシュ値を格納するＡＬＵ　ＲＡＭへアクセスするに際して、他の各処理を停止することにより、暗号化装置における瞬時電力のピークを低減された状態のもとに、公開鍵を用いた署名生成及び署名検証を高速且つ安全に行うことができる。

【０１３２】

また、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、使用するレジスタ群を時分割共用することにより、回路規模を削減して極めて少ない電力消費のもとに公開鍵を用いた署名生成及び署名検証を安全に行うことができる。

【０１３３】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号

化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用する。

【０１３４】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、使用するレジスタ群を時分割共用することにより、より回路規模と電力消費とを削減することができる。

【０１３５】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理コア手段と、ハッシュ値演算処理コア手段とを共用する。

【０１３６】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【０１３７】

したがって、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、演算処理に使用する演算処理コア手段を時分割共用し、また、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、バス切り替えスイッチを時分割共用することにより、さらに大幅な回路規模の削減と電力消費の削減とを図ることができる。

【０１３８】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【０１３９】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用することにより、より回路規模と電力消費とを削減することができる。

【０１４０】

さらに、この本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を格納する記憶手段を備え、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納する際に、公開鍵暗号化処理手段によって用いられるアドレスに当該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出す。

【０１４１】

したがって、本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡すことにより、回路規模及び電力消費の削減のみならず、処理の高速化も図ることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態として示す暗号化装置の概念を説明する図であって、（Ａ）は、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、（Ｂ）は、ＳＨＡ－１処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、（Ｃ）は、楕円曲線暗号化処理及びＳＨＡ－１処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用した様子を示す図である。

【図２】ＳＨＡ－１処理回路の具体的な実装例としての構成を説明するブロック図である。

【図３】ＳＨＡ－１処理回路の具体的な実装例としての他の構成を説明するブロック図である。

【図４】図２に示すＳＨＡ－１処理回路における基本動作を説明するためのフローチャートである。

【図５】図２に示すＳＨＡ－１処理回路における基本動作を説明するためのフローチャートであって、図４に示す工程に続く残りの工程を説明する図である。

【図６】楕円曲線暗号化処理回路の具体的な実装例としての構成を説明するブロック図である。

【図７】同楕円曲線暗号化処理回路の具体的な実装例としての要部構成を説明するブロック図であって、（Ａ）は、シフトレジスタ群における各シフトレジスタのうち、右側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示し、（Ｂ）は、シフトレジスタ群における各シフトレジスタのうち、左側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示す図である。

【図８】ＤＥＳ暗号化処理回路の具体的な実装例としての構成を説明するブロック図である。

【図９】同暗号化装置の具体的な実装例としての構成を説明するブロック図である。

【図１０】同暗号化装置を適用した非接触型ＩＣカードの構成を説明するブロック図である。

【図１１】同非接触型ＩＣカードにおける各部を機能的に表現したブロック図である。

【図１２】同非接触型ＩＣカードにおける時分割動作を説明するための図であり、（Ａ）は、通信モード時における動作を説明するためのブロック図であり、（Ｂ）は、楕円曲線暗号化処理モード時における動作を説明するためのブロック図であり、（Ｃ）は、ＤＥＳ暗号化処理モード時における動作を説明するためのブロック図であり、（Ｄ）は、ＡＬＵ　ＲＡＭモード時における動作を説明する

ためのブロック図である。

【図１３】同非接触型ＩＣカードにおける消費電力を説明するための図であり、（Ａ）は、ゲートにおける消費電力を説明する図であり、（Ｂ）は、ＡＬＵ　ＲＡＭアクセス時における消費電力を説明するための図であり、（Ｃ）は、ＲＡＭにおける消費電力を説明するための図であり、（Ｄ）は、該非接触型ＩＣカード全体の消費電力を説明するための図である。

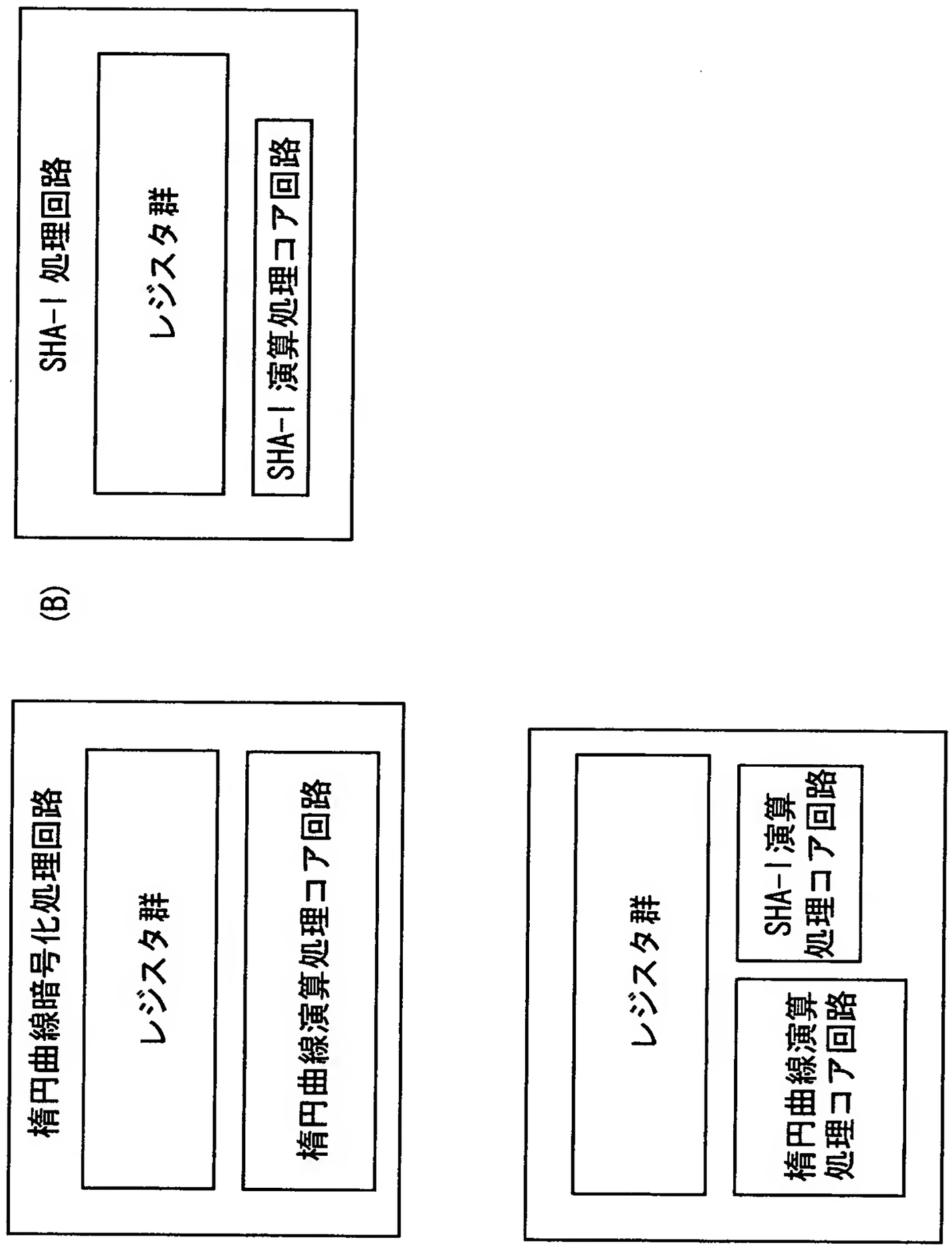
【図１４】従来の非接触型ＩＣカードにおける消費電力を説明するための図であり、（Ａ）は、ゲートにおける消費電力を説明する図であり、（Ｂ）は、ＡＬＵ　ＲＡＭアクセス時における消費電力を説明するための図であり、（Ｃ）は、ＲＡＭにおける消費電力を説明するための図であり、（Ｄ）は、該非接触型ＩＣカード全体の消費電力を説明するための図である。

【符号の説明】

１０，２０，５０，６０，７０，９０，１００，２００，２１０　シフトレジスタ群、　３０，２２０，３２０　ＲＯＭ、　４０，３７０　ＡＬＵ　ＲＡＭ、　８０　楕円曲線演算処理コア回路、　１１０　演算処理回路、　１２０　ＤＥＳ演算処理コア回路、　２３０　モンゴメリー演算回路、　３００　ＣＰＵ、　３１０　ＲＡＭ、　３３０　ＥＥＰＲＯＭ、　３４０　アナログブロック、　３５０　ＲＦブロック、　３６０　ＥＣＣ／ＳＨＡ１／ＤＥＳブロック、　360_1　ＥＣＣ／ＳＨＡ１ブロック、　360_2　ＤＥＳブロック、　３８０　テストブロック、　３９０　ＣＰＵインターフェース

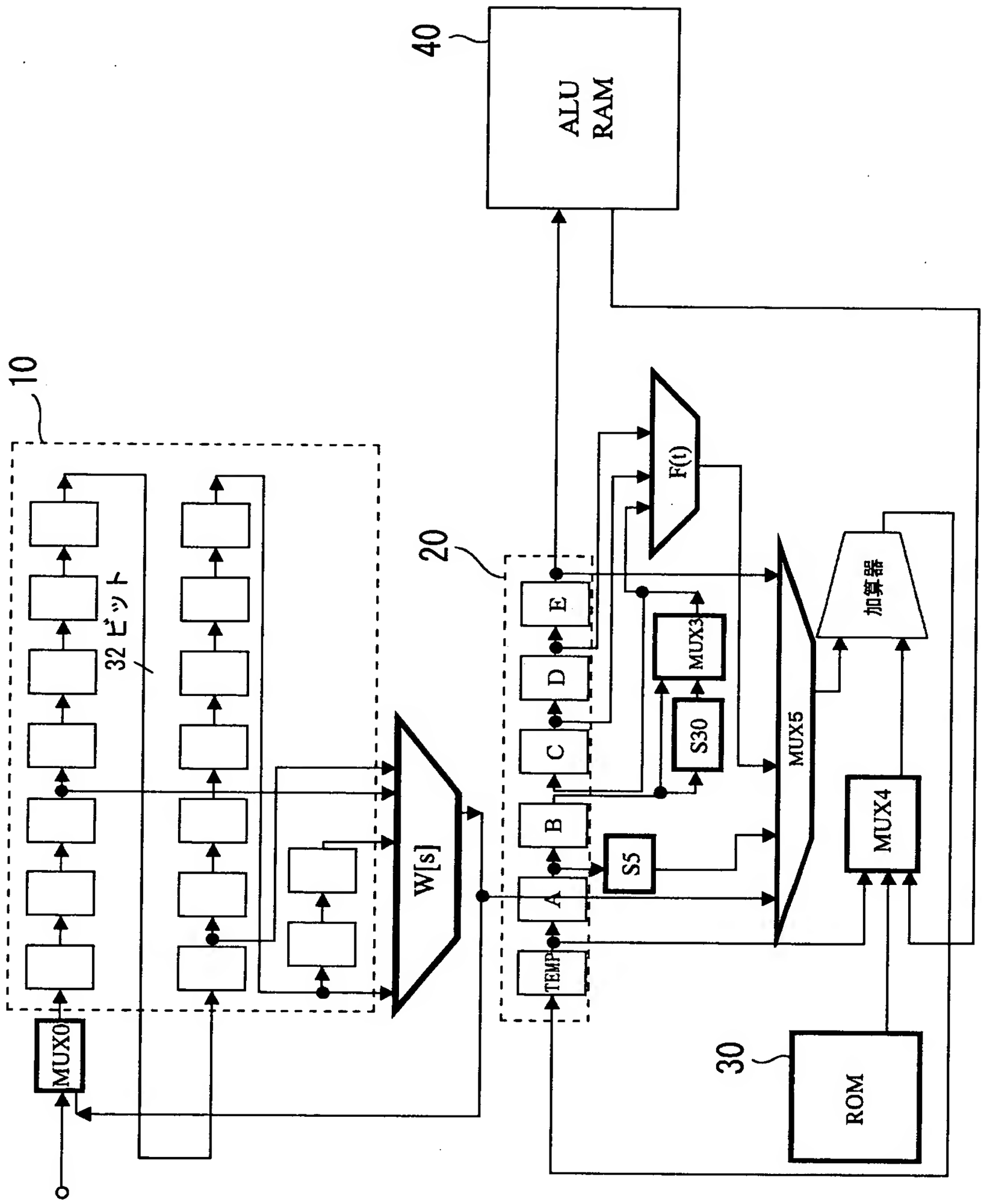
【書類名】　図面

【図１】



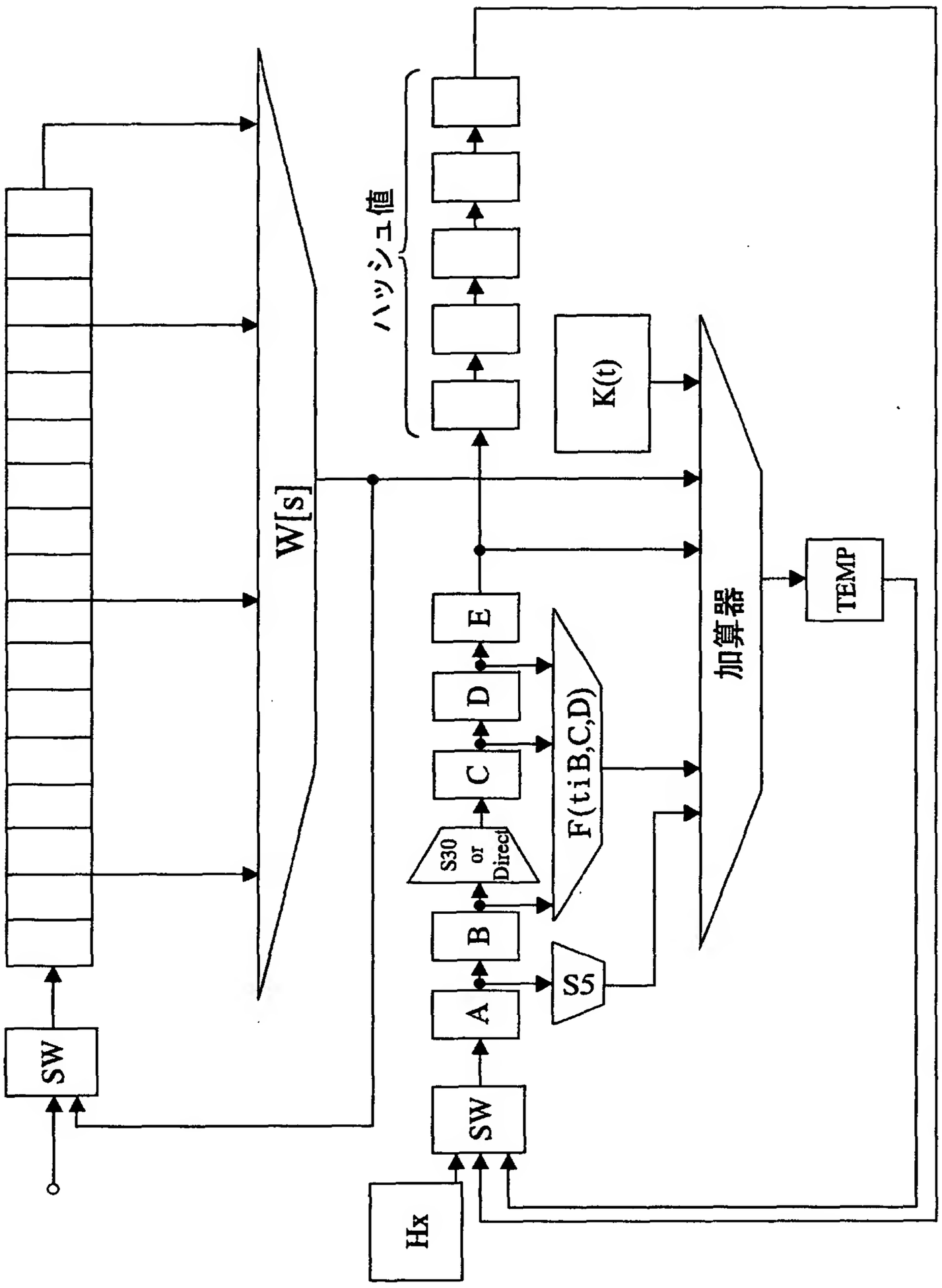
暗号化装置の概念図

【図２】



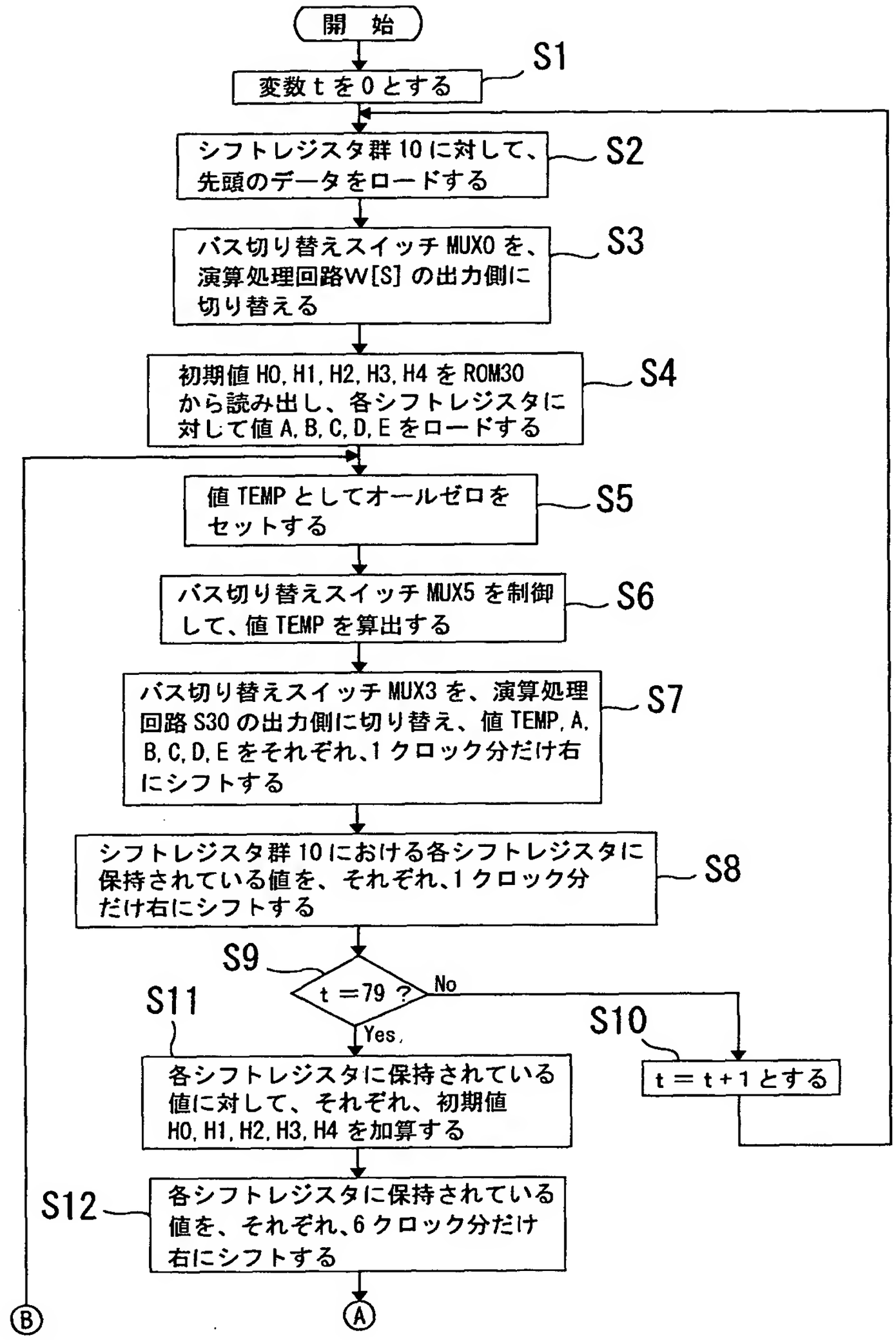
ＳＨＡ－１処理回路の構成ブロック図

【図３】



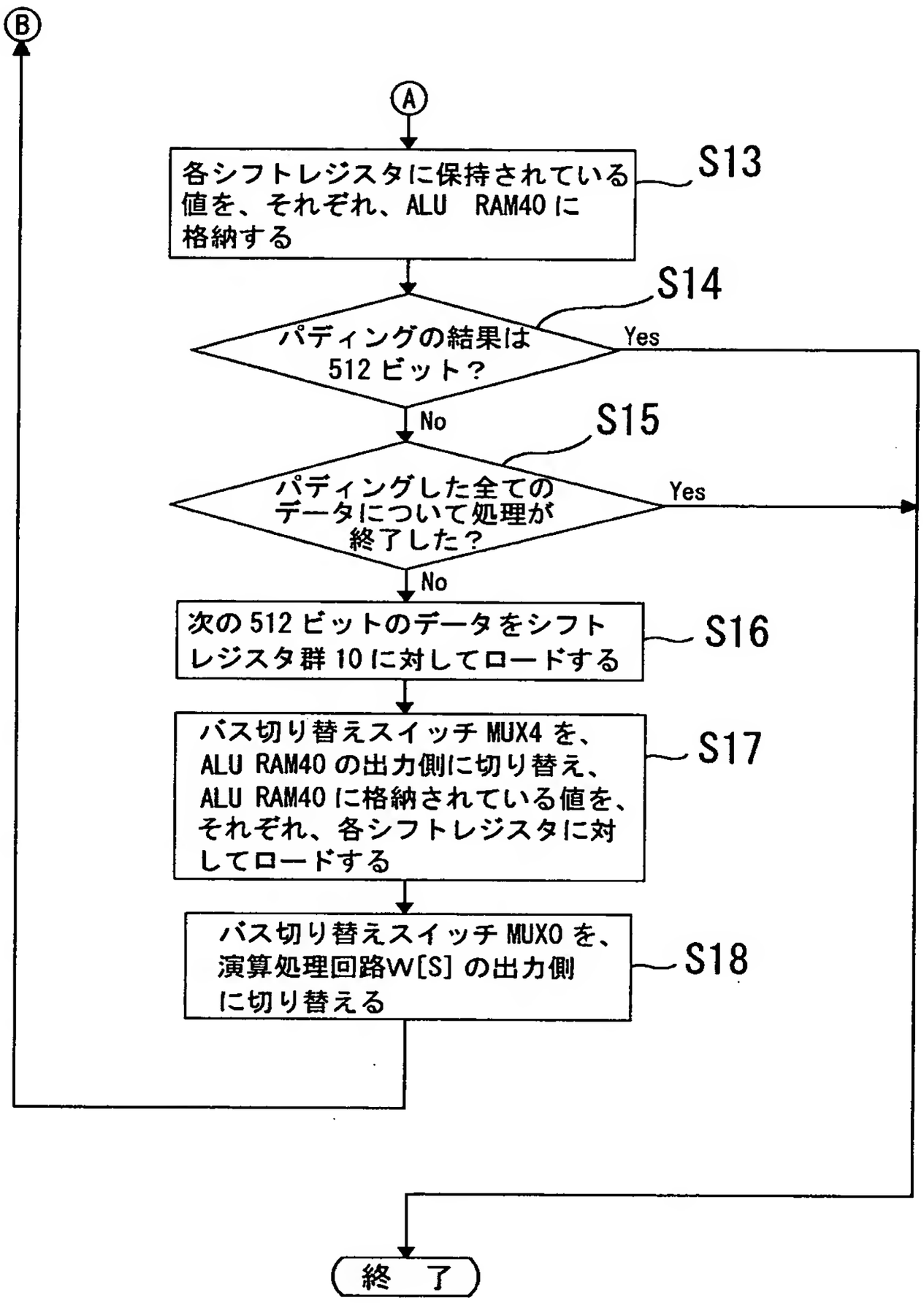
SHA－１処理回路の構成ブロック図

【図４】



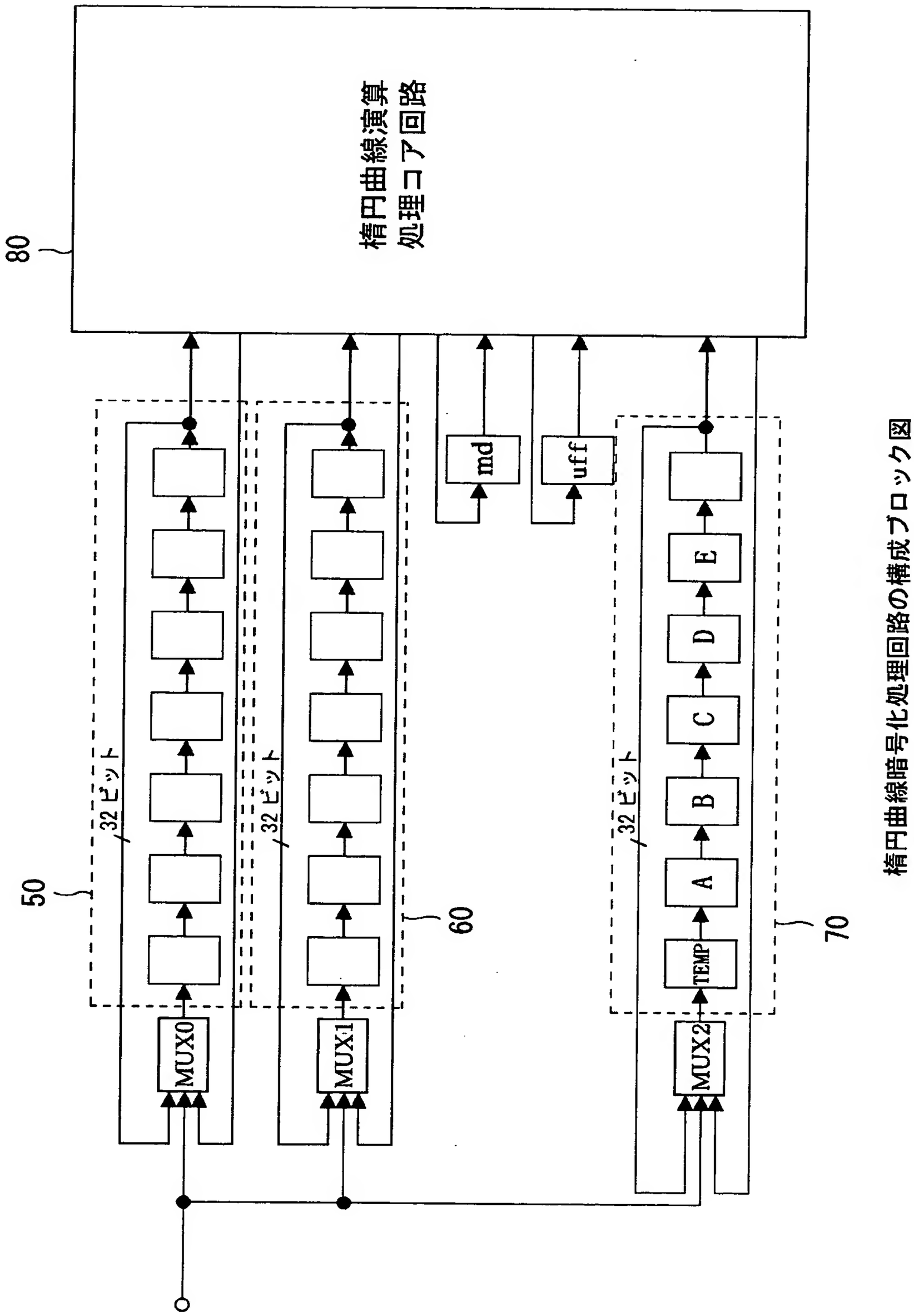
SHA－1 処理回路における一連の処理工程

【図５】



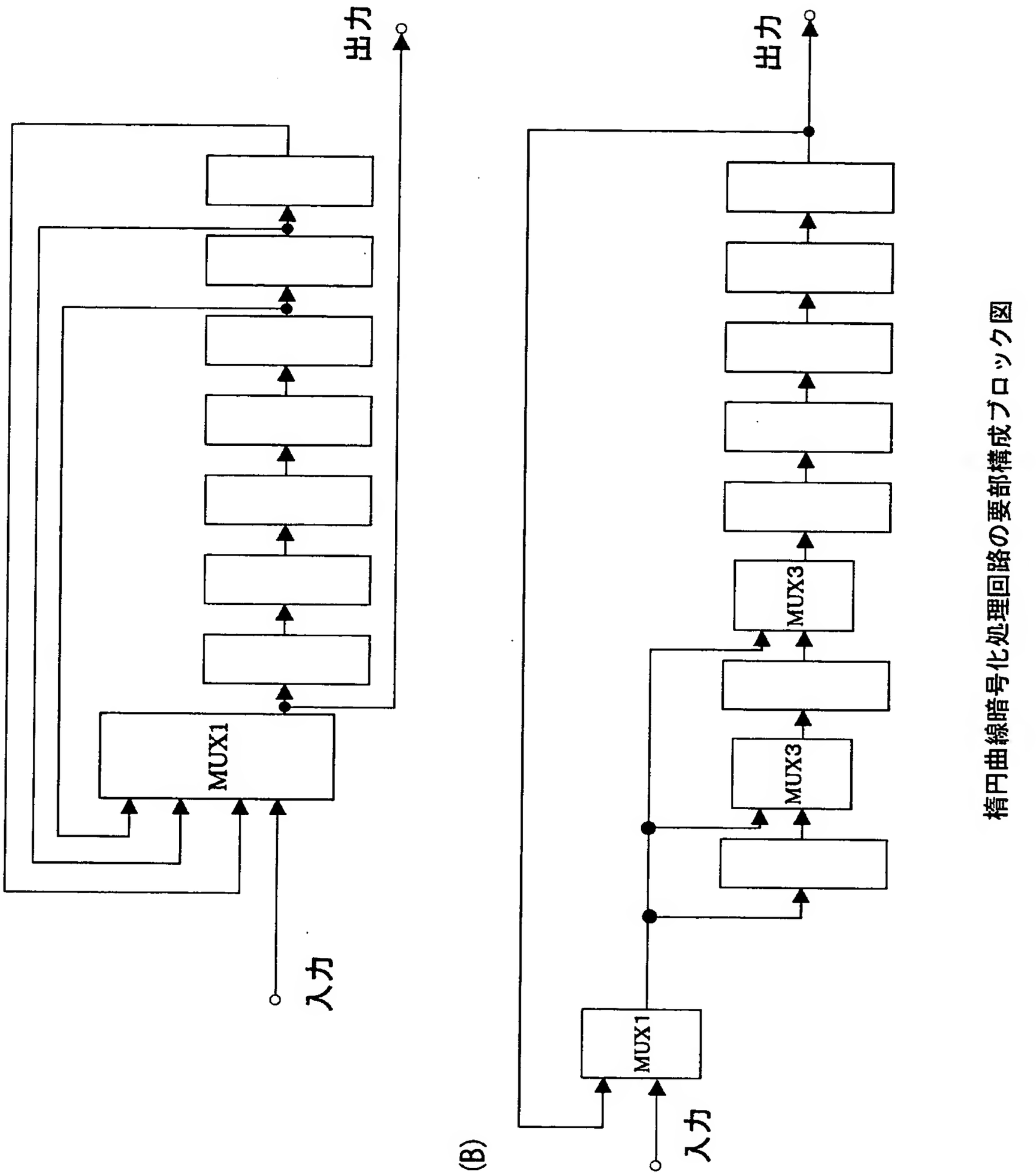
SHA－1 処理回路における一連の処理工程

【図６】



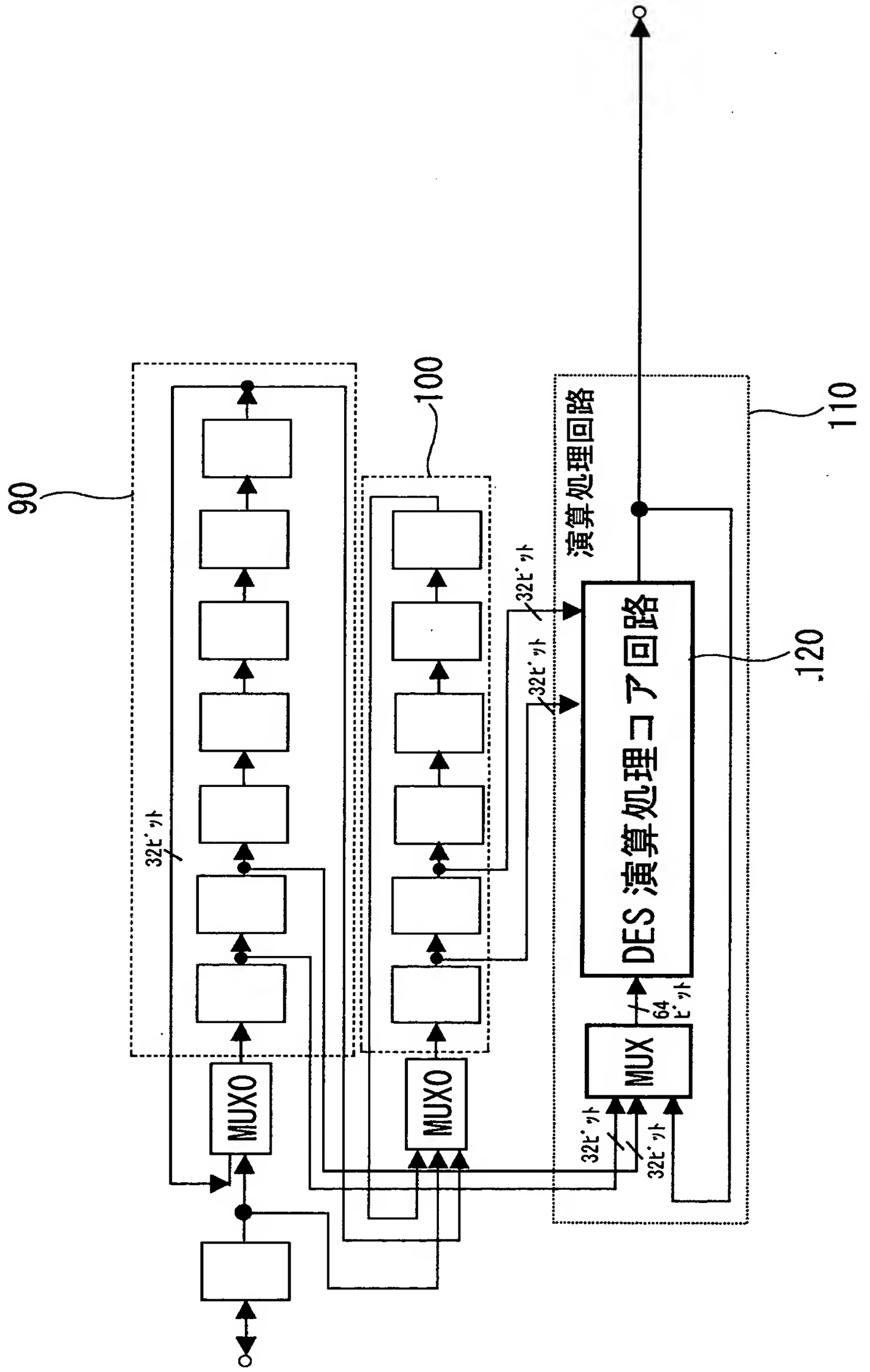
楕円曲線暗号化処理回路の構成ブロック図

【図７】



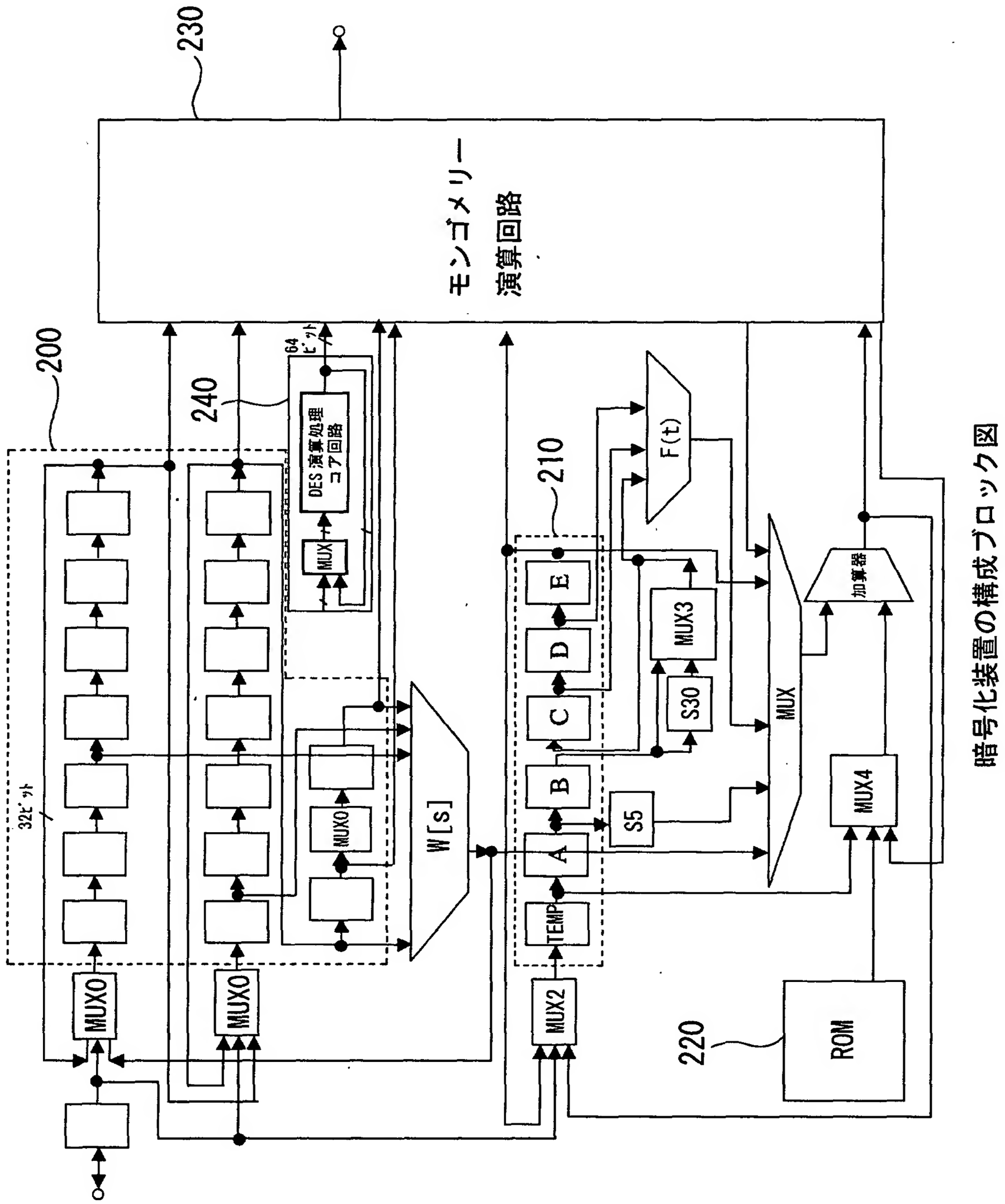
楕円曲線暗号化処理回路の要部構成ブロック図

【図８】



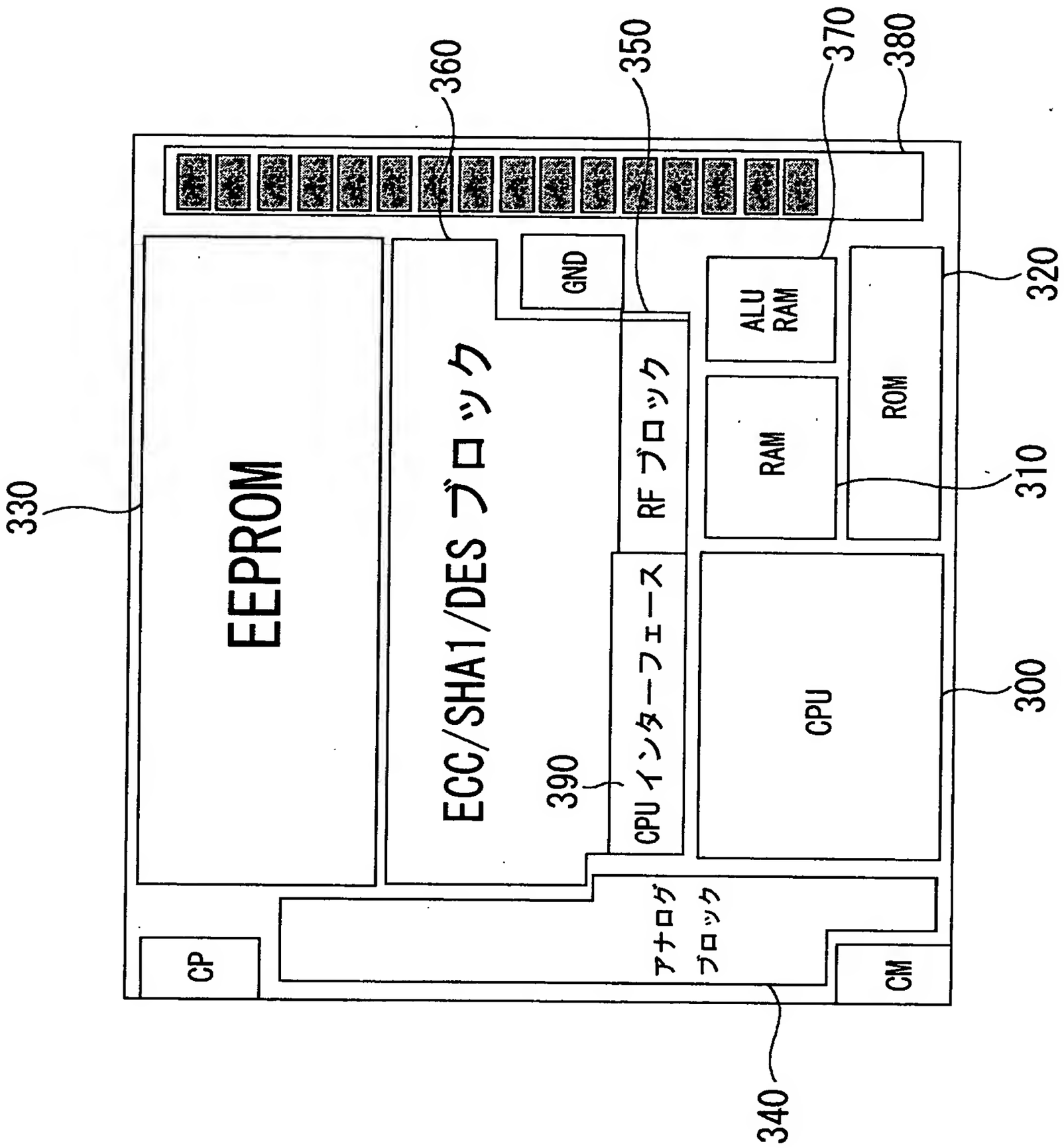
DES 暗号化処理回路の構成ブロック図

【図９】



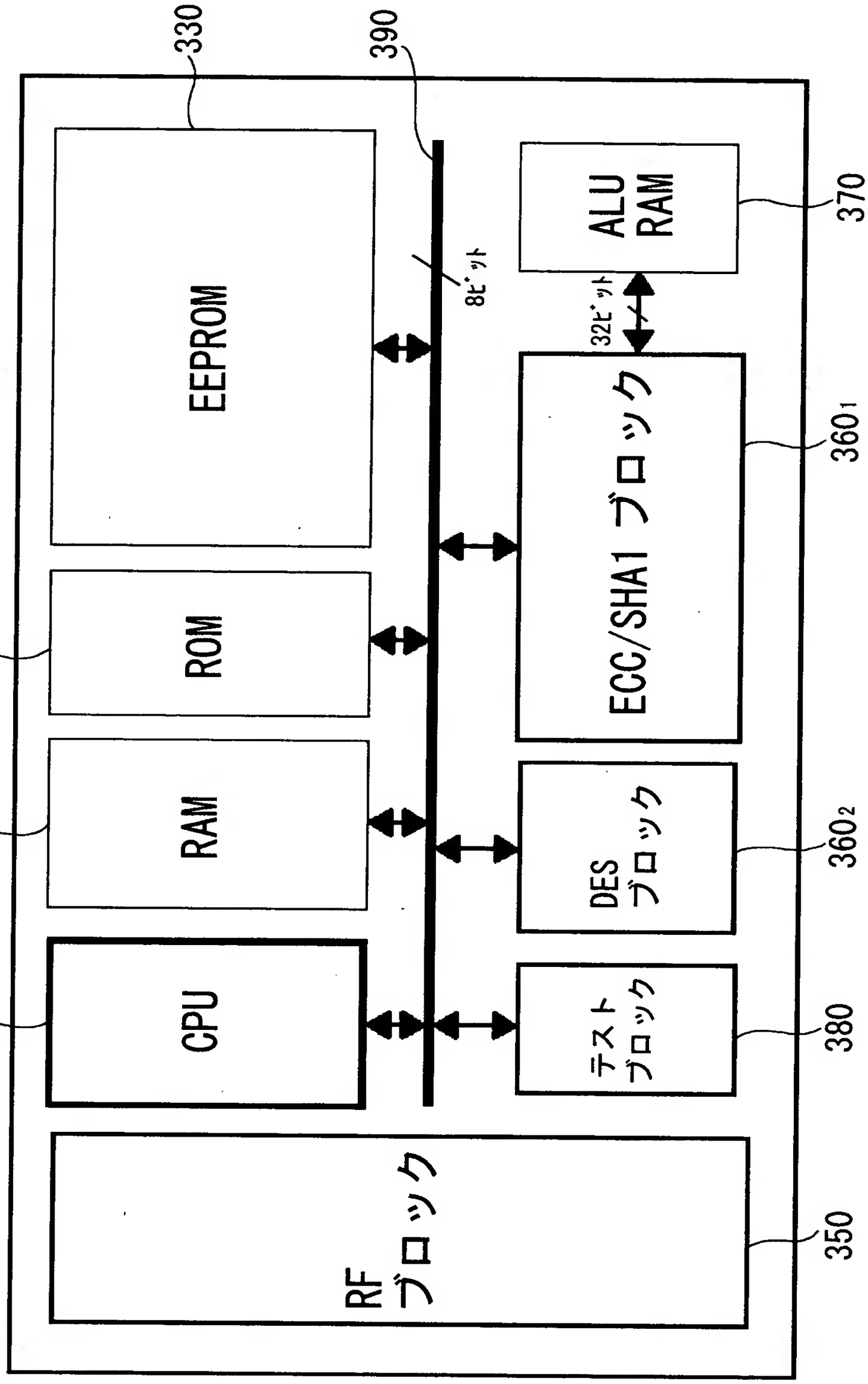
暗号化装置の構成ブロック図

【図１０】



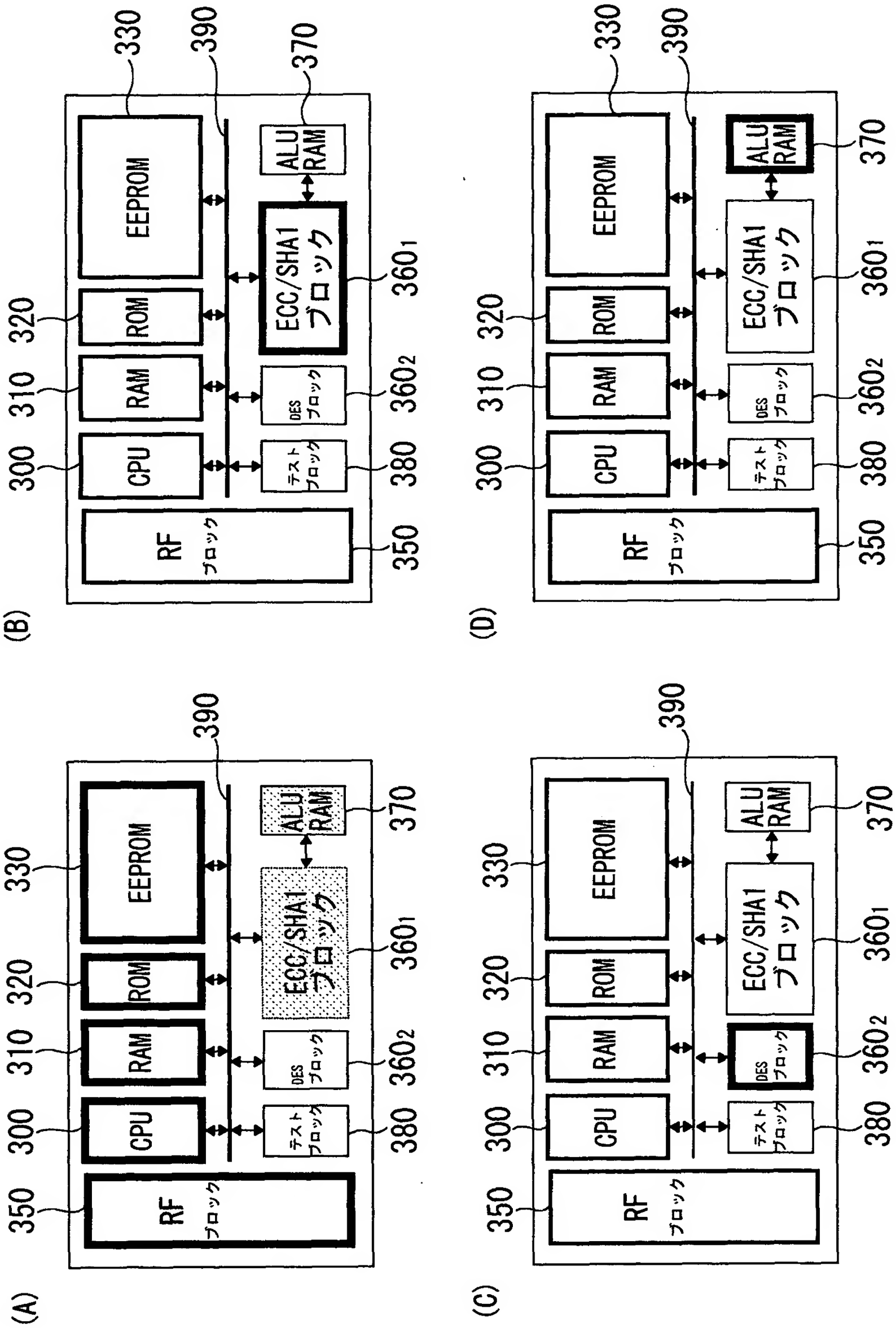
非接触型 IC カードの構成ブロック図

【図１１】



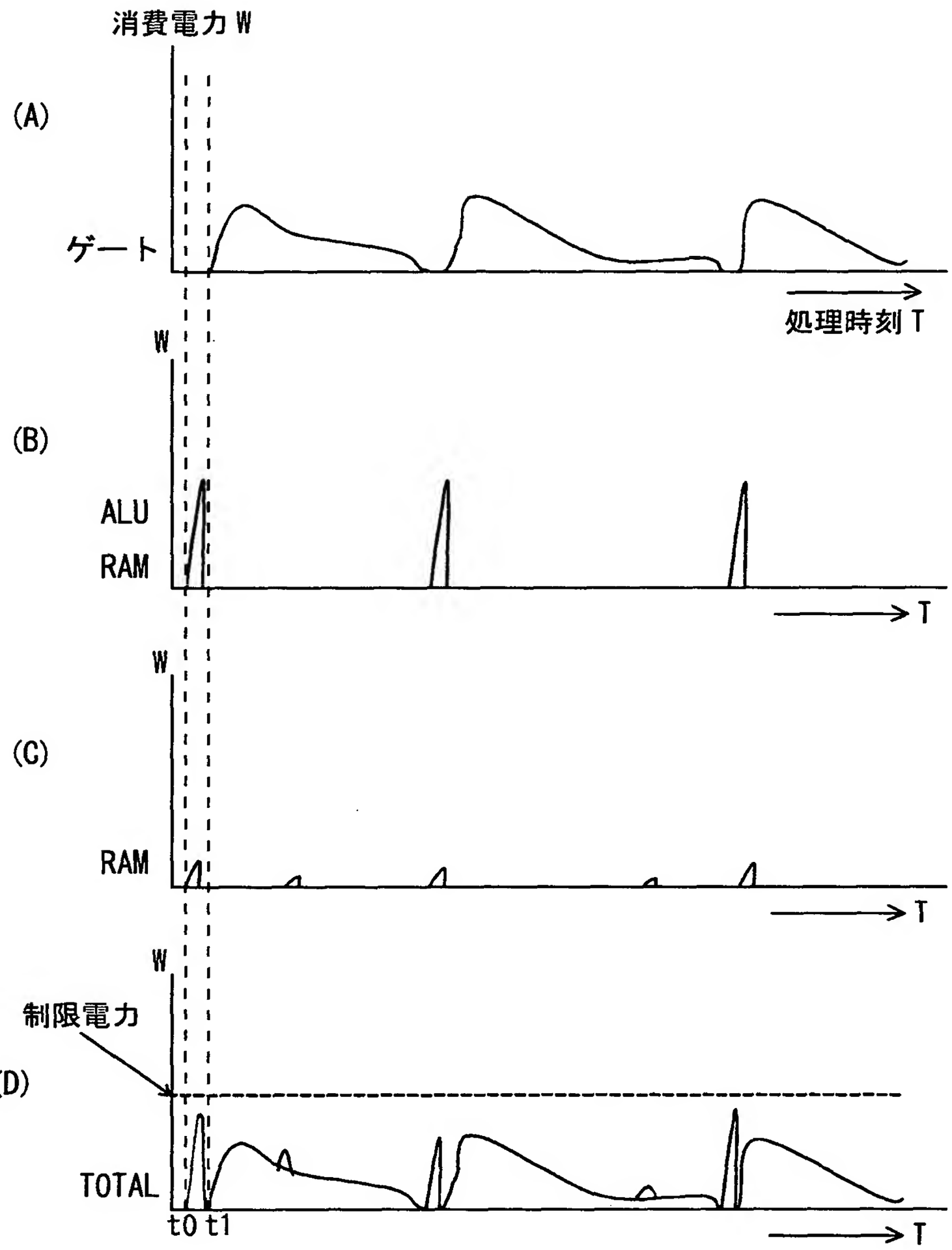
非接触型ICカードの構成ブロック図

【図１２】

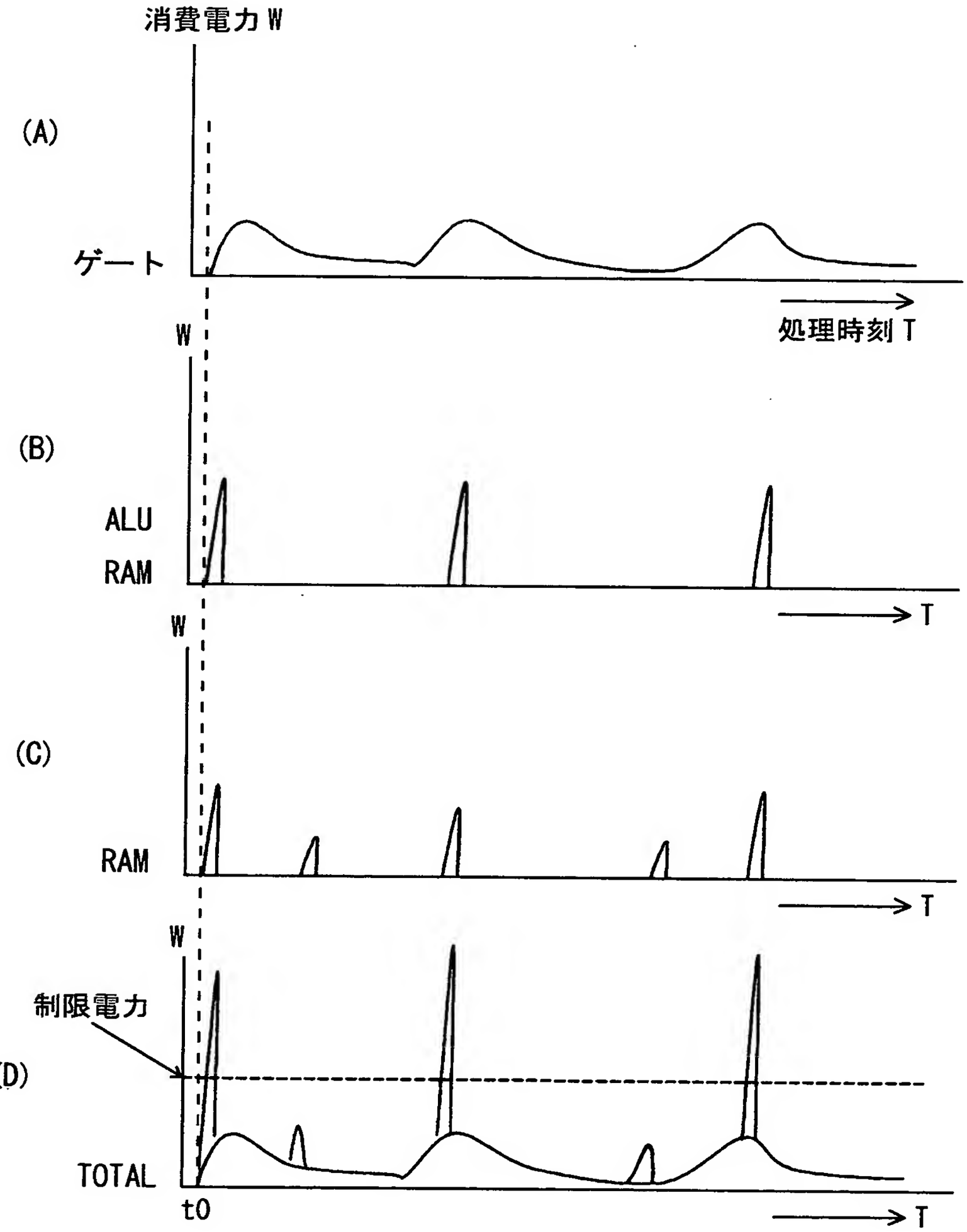


非接触型ICカードの動作の説明図

【図１３】



【図１４】



【書類名】　要約書

【要約】

【課題】　瞬時電力を低減することにより高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供する。

【解決手段】　本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限する。

【選択図】　図１２

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

２．変更年月日　　２００３年　５月１５日
［変更理由］　名称変更
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

出証特２００３－３０４４９３６